Bazylejski Komitet ds. Nadzoru Bankowego

Zasady zarządzania ryzykiem w bankowości elektronicznej

Maj 2001 r.

BANK ROZRACHUNKÓW MIĘDZYNARODOWYCH

Spis treści

Zasady zarządzania ryzykiem w bankowości elektronicznej

Streszczenie

Ciągłe innowacje technologiczne i konkurencja pomiędzy istniejącymi organizacjami bankowymi i instytucjami wchodzącymi na rynek umożliwiły klientom detalicznym i hurtowym dostęp do znacznie szerszego zakres usług i produktów bankowych oraz ich dostarczanie poprzez elektroniczny kanał dystrybucji, nazywany powszechnie bankowością elektroniczną. Jednak szybki rozwój możliwości bankowości elektronicznej niesie ze sobą zarówno korzyści jak i ryzyka.

Bazylejski Komitet ds. Nadzoru Bankowego oczekuje, iż instytucje bankowe będą identyfikowały, analizowały i w sposób ostrożnościowy zarządzały takimi ryzykami, zgodnie z podstawowymi cechami i wyzwaniami usług bankowości elektronicznej. Cechy te obejmują bezprecedensową szybkość zmian w zakresie innowacji technologicznych i obsługi klienta, wszechobecny, globalny charakter otwartych sieci elektronicznych, integrację aplikacji bankowości elektronicznej z pozostałymi systemami komputerowymi oraz rosnące uzależnienie banków od stron trzecich dostarczających niezbędnej technologii informatycznej. Komitet zauważył, że cechy te - nie tworząc całkowicie nowych ryzyk - zwiększyły i zmodyfikowały niektóre tradycyjne ryzyka związane z działalnością bankową, w szczególności ryzyko operacyjne, prawne i reputacji, wywierając przez to wpływ na ogólny profil ryzyka bankowości.

W oparciu o powyższe wnioski, Komitet sądzi, że obecne zasady zarządzania ryzykiem zachowują swą aktualność wobec elektronicznej działalności bankowej. Pomimo to, zasady te muszą być jednak odpowiednio dopasowane, dostosowane, a w niektórych wypadkach rozszerzone w celu ujęcia wyzwań wynikających z cech elektronicznej działalności bankowej. Komitet uważa, że realizacja tego celu zobowiązuje Rady Dyrektorów i wyższe kierownictwo banków do podejmowania działań zapewniających, że kierowane przez nie instytucje dokonają analizy i w razie konieczności zmodyfikują swą aktualną politykę i procesy zarządzania ryzykiem w sposób, który pozwoli na objęcie aktualnej i planowanej działalności w zakresie bankowości elektronicznej. Komitet sądzi także, że integracja aplikacji bankowości elektronicznej z pozostałymi systemami zakłada metodę zintegrowanego zarządzania ryzykiem w odniesieniu do całej działalności bankowej prowadzonej przez instytucję bankową.

W celu ułatwienia przeprowadzenia tych działań, Komitet sformułował 14 *Zasad zarządzania ryzykiem w bankowości elektronicznej*, które pomogą instytucjom bankowym rozszerzyć aktualnie stosowaną politykę i procesy kontroli ryzyka na ich działalność w zakresie bankowości elektronicznej.

Niniejsze *Zasady zarządzania ryzykiem* nie stanowią absolutnych wymogów lub nawet „najlepszej praktyki". Komitet sądzi, że ustalanie szczegółowych wymogów w zakresie zarządzania ryzykiem w obszarze bankowości elektronicznej może wywołać skutki przeciwne do zamierzonych, ponieważ wymogi te będą się prawdopodobnie szybko dezaktualizowały ze względu na tempo zmian w zakresie innowacji technologicznych i innowacji w zakresie obsługi klienta. Z tego względu, w celu promowania bezpieczeństwa i dobrego funkcjonowania bankowości elektronicznej, zachowując jednocześnie - po części w związku z tempem zmian w tym obszarze - konieczną elastyczność we wdrożeniu, Komitet wolał wyrazić oczekiwania i wskazówki nadzorcze w formie *Zasad zarządzania ryzykiem*. Ponadto, Komitet dostrzega fakt, że profil ryzyka każdego bank jest inny i wymaga dostosowania metody redukcji ryzyka do skali

operacji bankowości elektronicznej, istotności występujących ryzyk oraz woli i zdolności instytucji do zarządzania tymi ryzykami. Oznacza to, że metoda „jednego rozmiaru dla wszystkich" w zagadnieniach zarządzania ryzykiem w bankowości elektronicznej może nie być odpowiednia.

Z podobnego powodu *Zasady zarządzania ryzykiem* wydane przez Komitet nie usiłują ustanawiać konkretnych rozwiązań lub standardów technicznych dotyczących bankowości elektronicznej. Rozwiązania techniczne mają być w miarę rozwoju technologii opracowywane przez instytucje i organy ustalające standardy. Jednak niniejszy Raport zawiera załączniki zawierające przykłady aktualnie stosowanych i szeroko rozpowszechnionych praktyk redukcji ryzyka w bankowości elektronicznej, które mają charakter pomocniczy w stosunku do *Zasad zarządzania ryzykiem*.

Konsekwentnie, oczekuje się, że *Zasady zarządzania ryzykiem* i rzetelne praktyki określone w niniejszym Raporcie będą stosowane jako narzędzia przez krajowe instytucje nadzorcze i - w celu odzwierciedlenia specyficznych wymogów krajowych i indywidualnych profili ryzyka - wprowadzane z niezbędnymi adaptacjami. W niektórych obszarach, Zasady zostały wyrażone przez Komitet lub krajowe instytucje nadzorcze w poprzednich wskazówkach z zakresu nadzoru bankowego. Jednak niektóre zagadnienia, takie jak zarządzanie zlecaniem usług na zewnątrz [outsourcing], mechanizmy bezpieczeństwa i zarządzanie ryzykiem prawnym i ryzykiem reputacji wymagają bardziej szczegółowych zasad niż sformułowane do tej pory. Wynika to z unikalnych cech i implikacji internetowego kanału dystrybucji.

Zasady zarządzania ryzykiem można podzielić na trzy ogólne, a czasami nakładające się kategorie zagadnień, które są pogrupowane w celu zapewnienia przejrzystości: *Kontrola ze strony Rady i Kierownictwa; Kontrola bezpieczeństwa* i *Zarządzanie ryzykiem prawnym i ryzykiem reputacji.*

Kontrola ze strony Rady i Kierownictwa

Ponieważ Rada Dyrektorów i wyższe kierownictwo odpowiadają za opracowanie strategii gospodarczej instytucji oraz ustanowienie efektywnej kontroli ryzyka przez kierownictwo, oczekuje się podjęcia przez nie wyraźnej, dobrze ugruntowanej i udokumentowanej decyzji strategicznej dotyczącej tego czy i w jaki sposób bank będzie świadczył usługi bankowości elektronicznej. Wstępna decyzja powinna obejmować konkretne zakresy odpowiedzialności, politykę i instrumenty kontroli ryzyk, w tym ryzyk powstających w kontekście transakcji transgranicznych. Oczekuje się, że efektywna kontrola ze strony kierownictwa będzie obejmowała analizę i akceptację głównych aspektów procesu kontrolowania bezpieczeństwa banku, takich jak opracowanie i utrzymywanie infrastruktury kontroli bezpieczeństwa, we właściwy sposób zabezpieczającej systemy i dane bankowości elektronicznej przed zagrożeniami wewnętrznymi i zewnętrznymi. Powinna również obejmować wszechstronny proces zarządzania ryzykami wiążącymi się z rosnącą złożonością działalności i wzrastającym uzależnieniem od usług zlecanych na zewnątrz oraz stron trzecich w zakresie realizacji podstawowych funkcji bankowości elektronicznej.

Kontrola bezpieczeństwa

Pomimo, że Rada Dyrektorów jest odpowiedzialna za zapewnienie właściwych procesów kontroli bezpieczeństwa dla bankowości elektronicznej, istota tych procesów wymaga, ze względu na większe wyzwania dla bezpieczeństwa stawiane przez bankowość elektroniczną, szczególnej uwagi kierownictwa. Powinno to obejmować określenie odpowiednich przywilejów w zakresie upoważnień i środków weryfikowania tożsamości, instrumentów kontroli elektronicznego i fizycznego dostępu, adekwatnej infrastruktury bezpieczeństwa zachowującej odpowiednie granice i zastrzeżenia w stosunku do działań wewnętrznych i działań zewnętrznych użytkowników oraz rzetelności danych dotyczących transakcji, zapisów i informacji. Ponadto, należy zapewnić istnienie jasnych ścieżek audytu dla wszystkich transakcji bankowości elektronicznej. Środki służące zachowaniu poufności podstawowych informacji z zakresu bankowości elektronicznej powinny być adekwatne do poziomu wrażliwości tych informacji.

Pomimo różnic pomiędzy jurysdykcjami w zakresie regulacji dotyczących ochrony konsumenta i poufności informacji, banki ponoszą generalnie jasno określoną odpowiedzialność za zapewnienie swym klientom pewnego poziomu komfortu w zakresie udostępniania informacji, ochrony danych o nich oraz ich możliwości finansowych, na poziomie zbliżonym do poziomu, którego mogą oczekiwać korzystając z tradycyjnych bankowych kanałów dystrybucji.

Zarządzanie ryzykiem prawnym i ryzykiem reputacji

Aby ochronić banki przed ryzykiem gospodarczym, prawnym i ryzykiem reputacji, usługi bankowości elektronicznej muszą być dostarczane w sposób odpowiadający dużym oczekiwaniami klientów w zakresie ich stałej i szybkiej dostępności, a także przy potencjalnie wysokim popycie na transakcje. Bank musi być w stanie dostarczać usługi bankowości elektronicznej do wszystkich użytkowników końcowych i zachować tę zdolność w każdych okolicznościach. Duże znaczenie dla minimalizacji ryzyka operacyjnego, prawnego i ryzyka reputacji wynikającego z nieprzewidzianych zdarzeń, w tym z ataków wewnętrznych i zewnętrznych, mogących wpłynąć na dostarczanie systemów i usług bankowości elektronicznej, mają efektywne mechanizmy reagowania na incydenty. Z tego względu spełnianie oczekiwań klientów wymaga posiadania przez banki efektywnej zdolności świadczenia usług, ciągłości działalności gospodarczej oraz planowania awaryjnego. Banki powinny opracować również odpowiednie plany reagowania na incydenty, w tym strategie komunikacji, które zapewnią ciągłość działalności, kontrolowanie ryzyka reputacji oraz ograniczą odpowiedzialność związaną z zakłóceniami w dostarczanych przez bank usługach bankowości elektronicznej.

Raport *Zasady zarządzania ryzykiem w bankowości elektronicznej* jest przeznaczony do użytku publicznego. Uwagi ze strony organizacji bankowych i instytucji nadzoru bankowego są mile widziane i mogą być kierowane do Bazylejskiego Komitetu Nadzoru Bankowego za pośrednictwem faksu (+41 61 280 9100) lub poczty elektronicznej jean-philippe.svoronos@bis.org. Kopie uwag organizacji bankowych powinny być przekazane krajowym władzom nadzorczym, jeśli właściwe.

Zasady zarządzania ryzykiem w bankowości elektronicznej

I. Wstęp

Organizacje bankowe dostarczają usług elektronicznych konsumentom i podmiotom gospodarczym w sposób zdalny od lat. Elektroniczne przelewy środków, w tym płatności małej wartości i korporacyjne systemy zarządzania gotówką, jak również publicznie dostępne bankomaty służące do wypłaty środków i zarządzania rachunkami detalicznymi funkcjonują na całym świecie. Jednak rosnąca akceptacja Internetu[1] na całym świecie jako kanału dystrybucji produktów i usług bankowych zapewnia bankom nowe możliwości gospodarcze, a klientom korzyści w zakresie świadczonych im usług.

Ciągłe innowacje technologiczne i konkurencja pomiędzy istniejącymi organizacjami bankowymi i instytucjami wchodzącymi na rynek umożliwiły dostęp klientom detalicznym i hurtowym banków do znacznie szerszego zakresu usług i produktów bankowości elektronicznej[2]. Usługi te obejmują działalność tradycyjną, taką jak dostęp do informacji finansowej, uzyskiwanie pożyczek i otwieranie rachunków depozytowych, jak również produkty i usługi relatywnie nowe takie jak elektroniczne usługi płatności rachunków, osobiste „portale" finansowe, agregację rachunku[3] i możliwości zawierania bezpośrednich transakcji gospodarczych z kontrahentami lub poprzez giełdy.

Pomimo znacznych korzyści płynących z innowacji technologicznych, szybki rozwój możliwości bankowości elektronicznej niesie ze sobą również ryzyka. Istotna jest identyfikacja i ostrożnościowe zarządzanie tymi ryzykami przez instytucje bankowe[4]. Zagadnienia te skłoniły Bazylejski Komitet ds. Nadzoru Bankowego do przeprowadzenia w 1998 r. wstępnych badań w zakresie implikacji bankowości elektronicznej i pieniądza elektronicznego dla zarządzania ryzykiem[5]. To wstępne studium wykazało jasną potrzebę zintensyfikowania prac w obszarze

---

[1] Dla celów niniejszego Raportu, Internet obejmuje wszystkie technologie umożliwiające komunikację sieciową i otwarte sieci telekomunikacyjne od bezpośrednich połączeń telekomunikacyjnych, poprzez publiczną ogólnoświatową sieć WWW do wirtualnych sieci prywatnych.

[2] Dla celów niniejszego Raportu, bankowość elektroniczna [electronic banking lub ***e-banking***] obejmuje dostarczanie produktów i usług bankowych detalicznych i małej wartości poprzez kanały elektroniczne, jak również płatności elektroniczne dużej wartości i inne hurtowe usługi bankowe dostarczane drogą elektroniczną.

[3] Usługi agregacji rachunku umożliwiają klientom uzyskiwanie skonsolidowanej informacji o stanie ich rachunków finansowych i niefinansowych w jednym miejscu. Agregator działa zasadniczo jako agent klientów, dostarczający skonsolidowanych informacji na temat stanu rachunków klientów w kilku instytucjach finansowych. Klienci ujawniają agregatorowi konieczne hasło zabezpieczające lub osobisty numer identyfikacyjny umożliwiający dostęp i konsolidację informacji głównie poprzez gromadzenie danych wykazywanych na ekranie [screen scraping], proces obejmujący gromadzenie danych ze stron internetowych innych instytucji, często bez ich wiedzy, albo na podstawie umowy w sprawie bezpośredniego przekazywania danych pomiędzy instytucjami finansowymi.

[4] Ze względu na szybkie zmiany w technologii informatycznej, żaden opis takich ryzyk nie może być wyczerpujący. Jednak ryzyka, na które narażone są banki zaangażowane w bankowość elektroniczną, generalnie nie są nowe i zawierają się w kategoriach ryzyka określonych w *Podstawowych zasadach efektywnego nadzoru bankowego* Komitetu Bazylejskiego z września 1997 r. W wytycznych tych zidentyfikowano osiem kategorii ryzyka, w tym ryzyko kredytowe, ryzyko kraju i ryzyko transferu, ryzyko rynkowe, ryzyko stopy procentowej, ryzyko płynności, ryzyko operacyjne, ryzyko prawne i ryzyko reputacji. *Podstawowe zasady* są dostępne na stronie internetowej BIS http://www.bis.org.

[5] *„Zarządzanie ryzykiem w zakresie bankowej działalności elektronicznej i pieniądza elektronicznego"*, marzec 1998 r. Opracowanie dostępne na stronie internetowej Banku Rozrachunków Międzynarodowych http://www.bis.org.

zarządzania ryzykiem w bankowości elektronicznej. Misję tę powierzono Grupie ds. Bankowości Elektronicznej (EBG), grupie roboczej składającej się z instytucji nadzoru bankowego i banków centralnych, utworzonej w listopadzie 1999 r.

W październiku 2000 r.[6] Komitet Bazylejski wydał raport EBG w sprawie zarządzania ryzykiem i zagadnień nadzorczych wynikających z rozwoju bankowości elektronicznej. Raport ten dokonał inwentaryzacji i oceny głównych ryzyk związanych z bankowością elektroniczną, mianowicie: ryzyka strategicznego, ryzyka reputacji, ryzyka operacyjnego (w tym ryzyka zabezpieczeń i ryzyka prawnego)[7] oraz ryzyka kredytowego, rynkowego i płynności. Zgodnie z wnioskami EBG, działalność w zakresie bankowości elektronicznej nie powoduje powstania ryzyk nie zidentyfikowanych już w poprzednich pracach Komitetu Bazylejskiego. Jednak Grupa ustaliła, że bankowość elektroniczna zwiększa i modyfikuje charakter niektórych z tych tradycyjnych ryzyk, wpływając w ten sposób na ogólny profil ryzyka banku. W szczególności, szybki rozwój bankowości elektronicznej i stopień zaawansowania technologicznego tej działalności z pewnością zwiększa ryzyko strategiczne, ryzyko operacyjne i ryzyko reputacji.

A. Wyzwania dla zarządzania ryzykiem

EBG ustaliła, że podstawowe cechy bankowości elektronicznej (a bardziej ogólnie elektronicznej działalności handlowej) powodują szereg wyzwań dla zarządzania ryzykiem:

- Szybkość zmian w zakresie innowacji technologicznych i innowacji dotyczących obsługi klienta w bankowości elektronicznej jest bezprecedensowa. Z historycznego punktu widzenia nowe aplikacje bankowe były wprowadzane w ciągu relatywnie długich okresów czasowych oraz po dogłębnym przetestowaniu. Obecnie jednak banki doświadczają presji ze strony konkurencji na przygotowanie nowych aplikacji operacyjnych w bardzo ograniczonych ramach czasowych – częstokroć w ciągu zaledwie kilku miesięcy od koncepcji do produkcji. Konkurencja ta zwiększa stojące przed kierownictwem wyzwania w zakresie przeprowadzenia - przed wprowadzeniem nowych aplikacji bankowości elektronicznej - adekwatnej oceny strategicznej, analizy ryzyka i przeglądów zabezpieczeń.
- W celu prostszego przetwarzania transakcji elektronicznych, strony internetowe służące zawieraniu transakcji bankowości elektronicznej i związane z nimi aplikacje dla działalności detalicznej i hurtowej są zazwyczaj zintegrowana w najwyższym możliwym stopniu z pozostałymi systemami komputerowymi. Takie bezpośrednie zautomatyzowane przetwarzanie danych zmniejsza możliwości ludzkich błędów i oszustw stanowiących nieodłączny element transakcji ręcznych, zwiększa jednak uzależnienie od solidności zaprojektowania i architektury systemów, jak również od ich możliwości współpracy z innymi systemami, a także operacyjnej pojemności systemu.
- Bankowość elektroniczna zwiększa stopień uzależnienia banków od technologii informatycznej, zwiększając przez to techniczną złożoność wielu zagadnień operacyjnych i dotyczących zabezpieczeń i wzmacniając trend w kierunku większej liczby porozumień partnerskich, aliansów i umów o zlecanie usług ze stronami trzecimi, z których wiele nie jest regulowanych. Taki rozwój wydarzeń prowadzi do tworzenia nowych modeli działalności

[6] *„Inicjatywy Grupy ds. Bankowości Elektronicznej i Białe Księgi”*, październik 2000 r. Opracowanie dostępne na stronie internetowej BIS http://www.bis.org.

[7] Niniejszy Raport stosuje definicję ryzyka operacyjnego Grupy ds. Zarządzania Ryzykiem Komitetu Bazylejskiego, która obejmuje ryzyko zabezpieczeń i ryzyko prawne.

gospodarczej obejmujących banki i podmioty niebankowe, takie jak firmy dostarczające usług internetowych, spółki telekomunikacyjne i inne firmy technologiczne.

- Internet jest ze swej natury wszechobecny i ogólnoświatowy. Jest otwartą siecią dostępną z każdego miejsca na świecie przez nieznanych użytkowników, obejmującą przesyłanie informacji przez nieznane miejsca i za pośrednictwem szybko rozwijających się narzędzi bezkablowych. Z tego względu, znacznie zwiększa znaczenie kontrolnych mechanizmów zabezpieczających, technik potwierdzania tożsamości klienta, ochrony danych, procedur ścieżek audytu oraz standardów poufności danych o klientach.

B. Zasady zarządzania ryzykiem

Na podstawie wczesnych prac EBG, Komitet doszedł do wniosku, że pomimo, iż zasady zarządzania ryzykiem w tradycyjnej bankowości mają zastosowanie do bankowości elektronicznej, to złożone cechy elektronicznych kanałów dystrybucji wymagają, aby zasady te zostały dostosowane do wielu działań bankowości sieciowej i towarzyszącym im wyzwań w zakresie zarządzania ryzykiem. W związku z tym Komitet sądzi, że Rady Dyrektorów i wyższe kierownictwo banków są zobowiązane do podjęcia działań zapewniających, iż kierowane przez nie instytucje analizują i w miarę konieczności modyfikują stosowaną obecnie politykę i procesy zarządzania ryzykiem w sposób pozwalający na uwzględnienie bieżącej i planowanej działalności w zakresie bankowości elektronicznej. Następnie, ponieważ Komitet sądzi, że banki powinny przyjąć metodę zintegrowanego zarządzania ryzykiem obejmującego całą działalność bankową, bardzo ważne jest, aby kontrola zarządzania ryzykiem w zakresie bankowości elektronicznej stała się integralną częścią ogólnej struktury zarządzania ryzykiem przez instytucję bankową.

W celu umożliwienia takiego rozwoju wydarzeń, Komitet poprosił EBG o identyfikację podstawowych zasad zarządzania ryzykiem, które pomogłyby instytucjom bankowym rozszerzyć stosowaną przez nie politykę i procesy kontroli ryzyka na działalność w zakresie bankowości elektronicznej, co z kolei pozwoli promować bezpieczne i niezawodne dostarczanie produktów i usług bankowych drogą elektroniczną.

Niniejszych, określonych w Raporcie *Zasad zarządzania ryzykiem w bankowości elektronicznej* nie należy traktować jako absolutnych wymogów lub nawet „najlepszej praktyki", lecz raczej jako wskazówki mające na celu promowanie bezpiecznej i rzetelnej działalności w zakresie bankowości elektronicznej. Komitet sądzi, że ustalanie szczegółowych wymogów w zakresie zarządzania ryzykiem w obszarze bankowości elektronicznej może wywołać skutki przeciwne do zamierzonych, ponieważ wymogi te będą się prawdopodobnie szybko dezaktualizować ze względu na tempo zmian dotyczących technologii i produktów. Z tego względu, zasady przedstawione w niniejszym Raporcie wyrażają oczekiwania nadzorcze dotyczące realizacji ogólnego celu nadzoru bankowego polegającego na promowaniu bezpieczeństwa i dobrej kondycji systemu finansowego, a nie ścisłe regulacje.

Komitet reprezentuje pogląd, że takie oczekiwania nadzorcze należy przystosować do kanału dystrybucji bankowości elektronicznej. Jednocześnie, nie powinny się one różnić w sposób zasadniczy od oczekiwań wobec działalności bankowej realizowanej poprzez inne kanały dystrybucji. Wobec powyższego, przedstawione poniżej zasady zostały oparte w znacznym stopniu na zasadach nadzorczych wyrażanych przez Komitet lub krajowe instytucje nadzorcze w ciągu szeregu ostatnich lat. W niektórych obszarach, takich jak zarządzanie relacjami związanymi ze zlecaniem usług na zewnątrz, mechanizmy zabezpieczające oraz zarządzanie

ryzykiem prawnym i ryzykiem reputacji, cechy i implikacje internetowanego kanału dystrybucji wprowadzają potrzebę bardziej szczegółowego określenia zasad niż wyrażone do tej pory.

Komitet uznaje, że banki będą musiały opracować procesy zarządzania ryzykiem odpowiadające ich indywidualnemu profilowi ryzyka, strukturze operacyjnej i kulturze nadzoru korporacyjnego. Procesy te będą musiały być także zgodne ze szczególnymi wymogami i polityką w zakresie zarządzania ryzykiem, określonymi przez instytucje nadzorcze w ich jurysdykcji(-ach). Następnie, należy zauważyć, że wiele praktyk w obszarze zarządzania ryzykiem w bankowości elektronicznej, o których mowa w niniejszym Raporcie, jest odzwierciedleniem aktualnie stosowanej w sektorze rzetelnej praktyki. Nie należy wobec tego sądzić, że mają one charakter kompletny lub definitywny, ponieważ wiele mechanizmów kontrolnych i innych technik zarządzania ryzykiem ulega szybkim zmianom w związku z koniecznością nadążenia za nowymi technologiami i ich praktycznymi aplikacjami.

Niniejszy Raport nie usiłuje narzucać określonych rozwiązań technicznych dotyczących poszczególnych rodzajów ryzyka lub ustanawiać standardy techniczne dotyczące bankowości elektronicznej. Zagadnienia techniczne będą musiały być rozwiązywane w sposób ciągły przez instytucje bankowe i różne organy zajmujące się ustalaniem standardów w ślad za zmianami technologicznymi. Ponadto, jest prawdopodobne, że w miarę rozwiązywania przez sektor zagadnień technicznych w zakresie bankowości elektronicznej, w tym wyzwań dla bezpieczeństwa, pojawi się wiele innowacyjnych i efektywnych pod względem kosztów rozwiązań w zarządzaniu ryzykiem. Prawdopodobne jest także, że rozwiązania te uwzględnią zagadnienia związane z faktem, że banki różnią się co do rozmiaru, stopnia złożoności prowadzonej działalności i kultury zarządzania ryzykiem, a także z faktem występowania różnic prawnych i regulacyjnych pomiędzy jurysdykcjami.

Z tych powodów Komitet nie uważa, że metoda „jednego rozmiaru dla wszystkich" jest właściwa w bankowości elektronicznej, zachęca natomiast do wymiany dobrych praktyk i standardów uwzględniających dodatkowe wymiary ryzyka, będące wynikiem wykorzystywania kanału bankowości elektronicznej. Zgodnie z taką filozofią nadzorczą, oczekuje się, że zasady i rzetelne praktyki zarządzania ryzykiem określone w niniejszym Raporcie będą stosowane przez krajowe instytucje nadzorcze jako narzędzia, a następnie - z koniecznymi zmianami odzwierciedlającymi ewentualne specyficzne wymagania krajowe - wprowadzane w celu pomocy w promowaniu bezpiecznej i odpowiednio zabezpieczonej działalności oraz operacji bankowości elektronicznej.

Komitet dostrzega fakt, że profil ryzyka każdego bank jest inny i wymaga metody redukcji ryzyka odpowiadającej skali operacji bankowości elektronicznej, istotności obecnych ryzyk oraz woli i zdolności instytucji do zarządzania tymi ryzykami. Różnice te oznaczają, że zasady zarządzania ryzykiem przedstawione w niniejszym Raporcie mają być z zamierzenia wystarczająco elastyczne, aby mogły być wprowadzone przez wszystkie właściwe instytucje we wszystkich jurysdykcjach. Krajowe władze nadzorcze ocenią poziom istotności ryzyk związanych z bankowością elektroniczną występujących w danym banku, a także, czy i w jakim stopniu zasady zarządzania ryzykiem w bankowości elektronicznej są adekwatnie stosowane w systemie zarządzania ryzykiem tego banku.

II. Zasady zarządzania ryzykiem w bankowości elektronicznej

Zasady zarządzania ryzykiem w bankowości elektronicznej przedstawione w niniejszym Raporcie mogą być podzielone na trzy ogólne, czasami nakładające się kategorie. Jednakże, zasady te nie są ważone według jakichkolwiek preferencji lub znaczenia. Brak takiej hierarchii wynika z faktu, że waga poszczególnych zasad może się z czasem zmienić.

A. Kontrola ze strony Rady i Zarządu[8] (Zasady od 1 do 3):

1. Efektywna kontrola bankowości elektronicznej przez kierownictwo.
2. Ustanowienie wszechstronnego procesu kontroli bezpieczeństwa.
3. Wszechstronne zasady należytej staranności i kontrolowanie przez kierownictwo procesu zlecania usług na zewnątrz oraz innych rodzajów uzależnień od stron trzecich.

B. Mechanizmy kontroli bezpieczeństwa (Zasady od 4 do 10):

4. Sprawdzanie tożsamości klientów bankowości elektronicznej.
5. Uniemożliwienie negowania dokonanych transakcji oraz odpowiedzialność za transakcje bankowości elektronicznej.
6. Odpowiednie środki zapewniające podział obowiązków.
7. Właściwe mechanizmy kontroli upoważnień w ramach systemów, baz danych i aplikacji bankowości elektronicznej.
8. Rzetelność danych dotyczących transakcji, zapisów i informacji z zakresu bankowości elektronicznej.
9. Ustanowienie jasno określonych ścieżek audytu dla transakcji bankowości elektronicznej.
10. Poufność podstawowych informacji bankowych.

C. Zarządzanie ryzykiem prawnym i ryzykiem reputacji (Zasady od 11 do 14):

11. Odpowiednia sprawozdawczość dotycząca usług bankowości elektronicznej.
12. Poufność danych o klientach.
13. Pojemność systemu, zapewniania ciągłości działalności i planowanie awaryjne w celu zapewnienia dostępności systemów i usług bankowości elektronicznej.
14. Plany reagowania na incydenty.

Ponieważ zagadnienia te wiążą się z bankowością elektroniczną i podstawowymi zasadami zarządzania ryzykiem, które banki powinny rozważyć rozwiązując te zagadnienia,

[8] Niniejszy Raport odnosi się do struktury kierownictwa składającej się z rady dyrektorów oraz kierownictwa wyższego szczebla. Komitet jest świadom, że istnieją znaczne różnice w systemach regulacyjnych i prawnych poszczególnych krajów w zakresie funkcji rady dyrektorów i kierownictwa wyższego szczebla. W niektórych krajach główną funkcją rady, o ile nie wyłączną, jest nadzorowanie organu wykonawczego (kierownictwo wyższego szczebla, kierownictwo generalne). Z tego powodu, w pewnych przypadkach nazywa się ją radą nadzorczą. Oznacza to, że rada nie pełni żadnych funkcji wykonawczych. W innych krajach, przeciwnie, rada ma szersze kompetencje w tym sensie, iż określa sposób ogólnego zarządzania bankiem. Z powodu tych różnic, terminy „rada dyrektorów" i „zarząd" są używane w niniejszym Raporcie nie w celu identyfikacji różnych konstrukcji prawnych, lecz w celu odróżniania dwóch funkcji decyzyjnych w ramach banku.

każde z powyższych zagadnień omówiono w poniższych częściach. Tam, gdzie właściwe, w stosownych załącznikach zamieszczono rzetelne praktyki, które można rozważyć jako efektywne metody zarządzania tymi ryzykami.

A. Kontrola ze strony Rady i Zarządu (Zasady od 1 do 3)

Rada Dyrektorów i kierownictwo wyższego szczebla są odpowiedzialne za opracowanie strategii działalności gospodarczej instytucji bankowej. Przed zaoferowaniem usług bankowości elektronicznej należy podjąć jasną decyzję strategiczną, czy Rada chce, aby bank świadczył usługi dotyczące zawierania transakcji w ramach bankowości elektronicznej. W szczególności, Rada powinna upewnić się, czy plany dotyczące bankowości elektronicznej są wyraźnie zintegrowane ze strategicznymi celami korporacyjnymi, czy prowadzi się analizę ryzyka w zakresie proponowanej elektronicznej działalności bankowej, czy ustanowione są odpowiednie procesy redukowania i monitorowania zidentyfikowanych ryzyk oraz czy prowadzone są ciągłe analizy służące ocenie wyników bankowej działalności elektronicznej w odniesieniu do planów i celów instytucji.

Ponadto, Rada i wyższe kierownictwo powinny upewniać się, czy prawidłowo są rozważane i uwzględniane aspekty ryzyka operacyjnego i ryzyka zabezpieczeń realizowanej przez instytucję strategii gospodarczej elektronicznej działalności bankowej. Dostarczanie usług bankowych poprzez internet może w istotny sposób zmodyfikować i/lub nawet zwiększyć tradycyjne ryzyka bankowe (np. ryzyko strategiczne, ryzyko reputacji, ryzyko operacyjne, kredytowe i płynności). Z tego względu należy podjąć działania służące zapewnieniu właściwej oceny i wprowadzeniu odpowiednich zmian do istniejących procesów zarządzania ryzykiem w banku, procesów kontroli bezpieczeństwa, procesów należytej staranności i kontroli w zakresie zlecania usług na zewnątrz w celu ich dostosowania do usług bankowości elektronicznej.

Zasada 1: Rada Dyrektorów i kierownictwo wyższego szczebla powinny ustanowić efektywną kontrolę zarządczą ryzyk związanych z elektroniczną działalnością bankową, w tym ustanowić szczególne zasady rozliczania, polityki i kontroli służące zarządzaniu tymi ryzykami

Czujny nadzór ze strony kierownictwa ma podstawowe znaczenie dla zapewnienia efektywnych wewnętrznych mechanizmów kontroli elektronicznej działalności bankowej. Oprócz szczególnych cech internetowego kanału dystrybucji, omówionych we wstępie, znaczne wyzwanie dla tradycyjnych procesów zarządzania ryzykiem stanowią następujące aspekty bankowości elektronicznej:

- Główne elementy kanału dostarczania usług (internet i związane z nim technologie) znajdują się poza zasięgiem bezpośredniej kontroli banku.
- Internet ułatwia dostarczanie usług do wielu krajowych jurysdykcji, włącznie z tymi, które nie są obecnie obsługiwane przez fizyczne placówki instytucji.
- Ze względu na złożoność zagadnień związanych z bankowością elektroniczną, jak również wysoce techniczny język i pojęcia, kwestie związane z tą działalnością pozostają w wielu przypadkach poza tradycyjnym doświadczeniem Rady i kierownictwa wyższego szczebla.

W świetle unikalnych cech bankowości elektronicznej, nowe projekty w zakresie bankowości elektronicznej, które mogą wywrzeć istotny wpływ na profil ryzyka i strategię banku powinny być analizowane przez Radę Dyrektorów i kierownictwo wyższego szczebla oraz być poddawane odpowiednim analizom strategicznym i analizom kosztów / korzyści. Bez

dokonywania wstępnej analizy strategicznej i ciągłych ocen wyników w relacji do planu, występuje ryzyko niedoszacowania kosztów i/lub przeszacowania zysków wynikających z podejmowanych przez banki inicjatyw w zakresie bankowości elektronicznej.

Ponadto, Rada i kierownictwo wyższego szczebla powinny uniemożliwić podejmowanie przez bank nowej działalności w zakresie bankowości elektronicznej lub stosowanie nowych technologii bez posiadania koniecznej wiedzy zapewniającej kompetentną kontrolę zarządzania ryzykiem. Wiedza kierownictwa i pracowników powinna odpowiadać charakterowi technicznemu i poziomowi złożoności stosowanych w banku aplikacji bankowości elektronicznej i technologii bazowych. Adekwatna ekspertyza ma podstawowe znaczenie, bez względu na to, czy systemami i usługami bankowości elektronicznej zarządza sam bank, czy są zlecone osobom trzecim. W celu podejmowania efektywnych interwencji i rozwiązywania wszelkich istotnych ewentualnych problemów związanych z systemami bankowości elektronicznej lub przypadków naruszenia systemów bezpieczeństwa, procesy kontroli sprawowanej przez starsze kierownictwo powinny mieć charakter dynamiczny. Wiążące się z bankowością elektroniczną zwiększone ryzyko reputacji powoduje konieczność czujnego monitorowania zdolności funkcjonowania systemu i poziomu zadowolenia klientów, jak również konieczność zgłaszania ewentualnych incydentów do Rady i kierownictwa wyższego szczebla.

Wreszcie, Rada i kierownictwo wyższego szczebla powinny zapewnić integrację procesów zarządzania ryzykiem w bankowości elektronicznej ze stosowaną przez bank ogólną metodą zarządzania ryzykiem. Należy oceniać aktualną politykę i procesy zarządzania ryzykiem w celu upewnienia się, że są one wystarczająco sprawne, aby uwzględnić nowe ryzyka wynikające z prowadzonej lub planowanej elektronicznej działalności bankowej. Dodatkowe działania w zakresie zarządzania ryzykiem, które Rada i kierownictwo wyższego szczebla powinny rozważyć, obejmują:

- precyzyjne określenie akceptowanego przez organizację bankową poziomu ryzyka w zakresie bankowości elektronicznej,
- ustanowienie podstawowych upoważnień i mechanizmów podległości, w tym w odniesieniu do procedur zgłaszania przypadków wystąpienia incydentów wpływających na bezpieczeństwo, kondycję finansową lub reputację banku (np. przypadków penetracji sieci, złamania zasad bezpieczeństwa przez pracowników oraz wszelkich poważnych przypadków niewłaściwego użycia sprzętu komputerowego),[9]
- uwzględnienie unikalnych czynników ryzyka związanych z zapewnieniem bezpieczeństwa, integralności i dostępności produktów i usług bankowości elektronicznej oraz wymaganie, aby strony trzecie, którym banki zleciły sprawy podstawowych systemów lub aplikacji, podejmowały te same kroki,
- zapewnianie przeprowadzania odpowiednich analiz należytej staranności i analiz ryzyka przed rozpoczęciem prowadzenia przez bank transgranicznej elektronicznej działalności bankowej.

Internet znacznie zwiększa możliwości banku w zakresie dystrybucji produktów i usług na potencjalnie nieograniczonym terytorium geograficznym, przekraczającym granice krajów. Taka transgraniczna elektroniczna działalność bankowa prowadzona bez licencjonowanej fizycznej obecności w „kraju goszczącym” zwiększa ekspozycję banków na ryzyko prawne, regulacyjne i ryzyko kraju. Jest to skutkiem istotnych różnic pomiędzy jurysdykcjami, które

[9] Oprócz wymagań w zakresie wewnętrznego zgłaszania przypadków niewłaściwego użycia, procedury zgłaszania incydentów powinny określać obowiązki informacyjne wobec odpowiednich władz nadzorczych.

mogą występować w zakresie wymagań dotyczących licencjonowania, nadzoru i ochrony konsumenta. W związku z koniecznością unikania niezamierzonej niezgodności z ustawami i regulacjami kraju zagranicznego, jak również ze względu na konieczność zarządzania odpowiednimi czynnikami ryzyka kraju, banki rozważające prowadzenie transgranicznych operacji bankowości elektronicznej muszą - przed podjęciem takich operacji - dokonać gruntownej analizy tych ryzyk, a następnie efektywnie nimi zarządzać.

W zależności od zakresu i złożoności elektronicznej działalności bankowej, będą występowały różnice co do zakresu i struktury programów zarządzania ryzykiem w organizacjach bankowych. Zasoby wymagane do kontroli usług bankowości elektronicznej powinny odpowiadać poziomowi funkcjonalności i istotności systemów transakcyjnych, wrażliwości sieci oraz wrażliwości przekazywanych informacji.

Zasada 2: Rada Dyrektorów i kierownictwo wyższego szczebla powinny analizować i zatwierdzać podstawowe aspekty stosowanych w banku procesów kontroli bezpieczeństwa

Rada Dyrektorów i kierownictwo wyższego szczebla powinny nadzorować opracowanie i ciągłe funkcjonowanie infrastruktury kontroli bezpieczeństwa zapewniającej prawidłowe zabezpieczenie systemów i danych bankowości elektronicznej przed zagrożeniami wewnętrznymi i zewnętrznymi. Nadzór ten powinien obejmować nadawanie uprawnień, mechanizmy kontroli dostępu elektronicznego i fizycznego oraz adekwatną infrastrukturę zabezpieczającą, służącą zachowaniu odpowiednich ograniczeń dotyczących działań wewnętrznych i zewnętrznych użytkowników.

Ochrona aktywów banku stanowi jeden z podstawowych obowiązków powierzonych Radzie, jak również jest jednym z podstawowych obowiązków kierownictwa wyższego szczebla. Jednak, w szybko zmieniającym się środowisku bankowości elektronicznej, w związku ze złożonym ryzykiem zabezpieczeń, wynikającym z korzystania z sieci publicznie dostępnego internetu i stosowania innowacyjnych technologii, realizacja tego celu stanowi wyzwanie.

W celu zapewnienia odpowiednich systemów kontroli bezpieczeństwa elektronicznej działalności bankowej, Rada i kierownictwo wyższego szczebla muszą ustalić, czy bank posiada wszechstronny proces zabezpieczeń, w tym odpowiednią politykę i procedury, uwzględniające potencjalne wewnętrzne i zewnętrzne zagrożenia bezpieczeństwa. Dotyczy to zarówno zapobiegania incydentom, jak i odpowiedniego na nie reagowania. Podstawowe elementy efektywnego procesu zabezpieczenia bankowości elektronicznej obejmują:

- określenie wyraźnych obowiązków kierownictwa / pracowników w zakresie kontroli opracowywania i przestrzegania korporacyjnej polityki bezpieczeństwa,[10]
- odpowiednie zabezpieczenia fizyczne, zapobiegające dostępowi osób nieupoważnionych do sprzętu komputerowego,
- odpowiednie zabezpieczenia elektroniczne oraz procesy monitorowania dostępu[11], zapobiegające wewnętrznemu[12] i zewnętrznemu dostępowi do aplikacji i baz danych bankowości elektronicznej,

[10] Zazwyczaj obowiązki te nie powinny stanowić części funkcji audytu, który jest odpowiedzialny za kontrolowanie efektywnego wykonywania funkcji kontroli bezpieczeństwa.

[11] W tym uprawnienia i przywileje w zakresie kontrolowanego dostępu, jak również ciągłe monitorowanie prób uzyskania bezprawnego dostępu do sieci.

- regularne analizowanie i testowanie środków i mechanizmów kontroli bezpieczeństwa, w tym ciągłe śledzenie występujących w sektorze tendencji w zakresie zabezpieczeń oraz instalowanie odpowiednich nowych wersji oprogramowania, pakietów usług i innych wymaganych środków.[13]

W załączniku I przedstawiono szereg dodatkowych rzetelnych praktyk pomocnych w zapewnieniu bezpieczeństwa bankowości elektronicznej.

Zasada 3: Rada Dyrektorów i kierownictwo wyższego szczebla powinny ustanowić wszechstronny i ciągły proces badania należytej staranności i kontroli zarządzania zlecaniem usług na zewnątrz oraz innych zależności od stron trzecich wspierających bankowość elektroniczną

Zwiększające się uzależnienie od partnerów i usługodawców będących stronami trzecimi w zakresie wykonywania podstawowych funkcji osłabia bezpośrednią kontrolę ze strony kierownictwa banku. W związku z powyższym, konieczne jest wprowadzenie wszechstronnego procesu zarządzania ryzykami związanymi ze zlecaniem usług na zewnątrz oraz innymi rodzajami uzależnienia od stron trzecich. Proces ten powinien uwzględniać działalność partnerów i usługodawców będących stronami trzecimi, w tym zlecanie przez nich usług, mogących mieć istotny wpływ na bank, podwykonawcom.

W przeszłości, zlecanie usług na zewnątrz było ograniczone często do usługodawcy świadczącego jeden rodzaj usługi wiążącej się z określoną funkcją. Jednak w ostatnich latach, skala i poziom złożoności relacji banku z usługodawcami znacznie wzrosły. Jest to bezpośrednim wynikiem rozwoju technologii informatycznej i pojawienia się bankowości elektronicznej. Poziom złożoności tych relacji zwiększa ponadto fakt, że zlecone usługi bankowości elektronicznej mogą być następnie zlecane kolejnym podwykonawcom i/lub realizowane zagranicą. Następnie, ze względu na rosnący poziom zaawansowania technologicznego i strategicznego znaczenia aplikacji i usług bankowości elektronicznej, niektóre obszary funkcjonalne bankowości elektronicznej stały się uzależnione od małej liczby wyspecjalizowanych sprzedawców i usługodawców. Taki rozwój wydarzeń może prowadzić do zwiększonej koncentracji ryzyka, która zasługuje na uwagę zarówno z punktu widzenia indywidualnego banku jak i z punktu widzenia całego systemu.

Czynniki te wzięte razem podkreślają potrzebę wszechstronnej i ciągłej oceny relacji związanych ze zlecaniem usług na zewnątrz oraz innych rodzajów uzależnienia zewnętrznego, w tym skutków wynikających dla profilu ryzyka banku i możliwości kontroli zarządzania ryzykiem.[14] Prowadzona przez Radę i kierownictwo wyższego szczebla kontrola zlecania usług

---

[12] W tym pracowników, kontrahentów i osób upoważnionych do dostępu na podstawie umów dotyczących zlecania usług.

[13] W tym środków służących monitorowaniu funkcjonowania sieci, prób uzyskania bezprawnego elektronicznego dostępu oraz zgłaszania poważnych przypadków naruszenia bezpieczeństwa.

[14] Ocena taka powinna również uwzględniać poziom kontroli sprawowanej nad stroną trzeciej. W wielu przypadkach, główny akcjonariusz wspólnego przedsięwzięcia może, w oparciu o posiadany pakiet, sprawować znacznie większą kontrolę niż w oparciu o relację umowną z usługodawcą. Jednak, nie należy z powyższego rozróżnienia wnioskować, że kontrola działalności spółki sprawowana przez akcjonariusza musi być z konieczności dostateczna. Dotyczy to szczególnie sytuacji, w której technologie i usługi niezbędne do kierowania nią są dostarczane przez akcjonariusza mniejszościowego. Rozróżnienia takie są użyteczne przede wszystkim w celu potwierdzenia, że należy dokonywać oceny indywidualnych przypadków.

na zewnątrz i innego rodzaju uzależnień od stron trzecich powinna się koncentrować przede wszystkim na zapewnieniu:

- pełnego rozumienia przez bank ryzyk związanych z zawieraniem umów zlecania usług na zewnątrz i umów partnerskich dotyczących systemów i aplikacji bankowości elektronicznej,
- dokonywania, przed zawarciem jakiejkolwiek umowy dotyczącej usług bankowości elektronicznej, odpowiedniej analizy należytej staranności w zakresie kompetencji i sytuacji finansowej każdego usługodawcy – strony trzeciej lub partnera,
- jasnego zdefiniowania odpowiedzialności umownej stron umów w sprawie zlecania usług[15] lub porozumień partnerskich; np. należy w jasny sposób zdefiniować odpowiedzialność w zakresie udzielania informacji usługodawcom oraz uzyskiwania od nich informacji,
- zapewnienia, że wszystkie zlecone na zewnątrz systemy i operacje bankowości elektronicznej podlegają zarządzaniu ryzykiem i procedurom bezpieczeństwa i poufności spełniających własne standardy banku,
- zapewnienia okresowych niezależnych audytów wewnętrznych i/lub zewnętrznych zleconych operacji, obejmujących co najmniej taki sam zakres jaki jest wymagany w przypadku operacji prowadzonych na miejscu,
- istnienia odpowiednich planów awaryjnych dla zleconych działań bankowości elektronicznej.

W Załączniku II przedstawiono szereg dodatkowych, rzetelnych praktyk dotyczących zarządzania zleconymi na zewnątrz systemami bankowości elektronicznej oraz innymi rodzajami zależności od stron trzecich.

B. Mechanizmy kontroli bezpieczeństwa (Zasady od 4 do 10)

Pomimo odpowiedzialności Rady Dyrektorów za zapewnienie odpowiednich procesów kontroli bezpieczeństwa w zakresie bankowości elektronicznej, istota tych procesów wymaga szczególnej uwagi ze strony kierownictwa, ponieważ bankowość elektroniczna zwiększa wyzwania w zakresie bezpieczeństwa.[16] W szczególności istotne są następujące zagadnienia:

- potwierdzenie tożsamości (uwierzytelnienie),
- uniemożliwienie zaprzeczania realizacji transakcji,
- integralność danych i transakcji,
- podział obowiązków,
- kontrola upoważnień,
- zachowanie ścieżek audytu,
- poufność podstawowych informacji bankowych.

[15] Powyższe winno także obejmować podwykonawców.

[16] Na przykład, jeśli w zakresie usług bankowości elektronicznej Rada polega na usługodawcach będących stronami trzecimi, to musi upewnić się, że usługodawca w adekwatny sposób rozwiązał te zagadnienia oraz, że spełnia własne standardy banku.

Zasada 4: Banki powinny podjąć odpowiednie kroki w celu potwierdzenia tożsamości[17] i upoważnień klientów, z którymi prowadzą interesy za pośrednictwem internetu

Podstawowe znaczenie w bankowości ma potwierdzenie, czy dana próba kontaktu, transakcji lub dostępu jest uprawniona. Zgodnie z powyższym, banki powinny stosować niezawodne metody weryfikowania tożsamości i upoważnień nowych klientów, jak również potwierdzenia tożsamości i uprawnień aktualnych klientów dążących do zainicjowania transakcji elektronicznych.

Weryfikacja klienta przy otwieraniu rachunku jest ważna, ponieważ zmniejsza ryzyko podszywania się pod inną osobę, oszukańczego wykorzystania rachunku i prania pieniędzy. Wynikiem braku adekwatnego potwierdzenia tożsamości klientów przez bank może być uzyskanie przez nieuprawnione osoby dostępu do rachunków bankowości elektronicznej i ostatecznie strata finansowa lub zaszkodzenie reputacji banku poprzez oszustwo, ujawnienie informacji poufnych lub mimowolne zaangażowanie w działalność kryminalną.

Stwierdzenie i potwierdzenie tożsamości i uprawnień osoby do dostępu do systemów bankowych w środowisku czysto elektronicznej otwartej sieci może być zadaniem trudnym. Uprawnienia użytkownika mogą być fałszywie przedstawione poprzez rozmaite techniki znane ogólnie jako „spoofing”[18]. Hakerzy sieciowi mogą także przejąć sesję uprawnionej, upoważnionej osoby poprzez zastosowanie urządzenia zwanego „sniffer”[19] i prowadzić działania o charakterze szkodliwym lub kryminalnym. Procesy kontroli uwiarygodniania tożsamości mogą być także obchodzone poprzez zmianę baz danych dotyczących potwierdzania tożsamości.

Zgodnie z powyższym, podstawowe znaczenie ma posiadanie przez banki formalnej polityki i procedur określających odpowiednią(-e) metodologię(-e) zapewniającą(-e) właściwe potwierdzanie przez bank tożsamości i upoważnienia osoby, agenta lub systemu[20] za pomocą środków, które są unikalne i, w praktycznym stopniu, wyłączają nieupoważnione osoby lub systemy.[21] Banki mogą korzystać z różnych metod ustalania tożsamości, w tym osobistego numeru identyfikacyjnego PIN, haseł, kart smart, danych biometrycznych i certyfikatów cyfrowych.[22] Metody te mogą się opierać na jednym czynniku lub wielu czynnikach (np. stosowanie w celu potwierdzenia tożsamości zarówno hasła jak i technologii biometrycznej[23]).

---

[17] Termin *potwierdzenie tożsamości, uwiarygodnienie,* [authentication] jest używany w niniejszym Raporcie dla oznaczenia technik, procedur i procesów weryfikowania tożsamości i uprawnień obecnych i przewidywanych klientów. Termin *identyfikacja* [identification] oznacza procedury, techniki i procesy stosowane do stwierdzania tożsamości klienta w momencie otwierania rachunku. Termin *upoważnienie, autoryzacja* [authorisation] oznacza procedury, techniki i procesy stosowane w celu ustalenia, czy klient lub pracownik posiada prawo dostępu do rachunku bankowego lub prawo do dokonywania transakcji na tym rachunku.

[18] Spoofing polega na odpersonifikowaniu klienta poprzez wykorzystanie jego numeru rachunku, hasła, osobistego numeru identyfikacyjnego (PIN) i/lub adresu poczty elektronicznej.

[19] Sniffer jest urządzeniem zdolnym do podsłuchiwania ruchu telekomunikacyjnego, przejmowania przesyłanych haseł i danych.

[20] Systemy obejmują także własne strony internetowe instytucji.

[21] Systemy muszą gwarantować, że prowadzą operacje z uprawnioną osobą, agentem lub systemem i stosują właściwą bazę danych dotyczących potwierdzania tożsamości.

[22] Bank może wydawać certyfikaty cyfrowe przy zastosowaniu publicznego klucza dostępu do infrastruktury [public key infrastructure] (PKI) do klienta w celu zabezpieczenia komunikacji z bankiem. Certyfikaty cyfrowe i PKI są omówione w większych szczegółach w Zasadzie 5.

[23] Technologia biometryczna jest automatycznym badaniem fizjologicznych lub behawioralnych cech używanych do identyfikacji i/lub potwierdzenia tożsamości osoby. Pospolite rodzaje technologii biometrycznej obejmują

Stosowanie wieloczynnikowego potwierdzenia tożsamości gwarantuje zazwyczaj większą wiarygodność.

W oparciu o dokonaną przez kierownictwo ocenę ryzyka powodowanego przez system bankowości elektronicznej jako całość lub jego różne części składowe, Bank musi ustalić metody potwierdzania tożsamości, które będzie stosował. Taka analiza ryzyka ocenia możliwości transakcyjne[24] systemu bankowości elektronicznej (np. przelew środków, opłacanie rachunków, złożenie wniosku o pożyczkę, agregacja rachunku, etc.), wrażliwość i wartość przechowywanych danych bankowości elektronicznej oraz łatwość korzystania przez klienta z metody potwierdzenia tożsamości.

Biorąc pod uwagę dodatkowe trudności, które mogą wynikać z elektronicznego prowadzenia interesów z klientami poza granicami krajowymi, w tym zwiększone ryzyko odpersonifikowania tożsamości i zwiększoną trudność sprawdzania zdolności kredytowej potencjalnych klientów, efektywne procesy identyfikacji i potwierdzenia tożsamości są szczególnie ważne w kontekście elektronicznej bankowości transgranicznej.

W miarę ciągłej ewolucji metod potwierdzania tożsamości zachęca się banki do monitorowania i przyjmowania rzetelnych praktyk stosowanych przez sektor w tym obszarze zapewniających, że:

- Bazy danych dotyczących tożsamości, zapewniające dostęp do rachunków klientów bankowości elektronicznej lub systemów wrażliwych są chronione przed manipulacjami i korupcją. Każda próba manipulacji powinna być wykrywalna i powinny istnieć ścieżki audytu pozwalające na dokumentację takich prób.
- Każde przypadek dodania, usunięcia lub zmiany danych o osobie, agencie lub systemie w bazie danych dotyczących tożsamości jest należycie autoryzowany przez upoważnione źródło.[25]
- Stosowane są odpowiednie środki kontroli połączenia systemu bankowości elektronicznej, które uniemożliwiają nieznanym stronom trzecim podszywanie się pod znanych klientów.
- Zatwierdzone sesje bankowości elektronicznej pozostają bezpieczne w ciągu całego okresu ich trwania, ewentualnie - w przypadku upływu zabezpieczenia - sesja powinna wymagać ponownego zatwierdzenia.

Zasada 5: Banki powinny stosować takie metody potwierdzania transakcji, które uniemożliwiają negowanie dokonanych transakcji i wprowadzają odpowiedzialność za transakcje bankowości elektronicznej

Uniemożliwienie negowania zrealizowanych transakcji obejmuje stworzenie dowodu dotyczącego pochodzenia lub miejsca przeznaczenia informacji elektronicznej w celu ochrony

---

skanowanie twarzy, skanowanie odcisków palców, skanowanie tęczówki oka, skanowanie siatkówki oka, skanowanie dłoni, skanowanie podpisu, skanowanie głosu i dynamikę uderzeń w klawiaturę. Systemy identyfikacji biometrycznej zapewniają bardzo wysoki poziom uwiarygodnienia, mogą być jednak trudniejsze do wdrożenia niż inne metody identyfikacji / uwiarygodnienia.

[24] Efektywne środki potwierdzania tożsamości mogą również zmniejszać ryzyko negowania dokonanych transakcji, w którym upoważniony użytkownik zaprzecza po dokonaniu transakcji jakoby jej wcześniej dokonał (zobacz także Zasada 5).

[25] W niektórych przypadkach upoważnione źródło może być źródłem elektronicznym.

wysyłającego informacje przed fałszywym zanegowaniem otrzymania danych przez otrzymującego informację, lub ochrony otrzymującego informację przed fałszywym potwierdzeniem wysyłki informacji przez wysyłającego. Ryzyko negowania transakcji występuje już w konwencjonalnych transakcjach, takich jak karty kredytowe i transakcje papierami wartościowymi. Jednak, bankowość elektroniczna zwiększa to ryzyko z powodu trudności w pozytywnym potwierdzeniu tożsamości i uprawnień stron inicjujących transakcje, możliwości zmiany lub przejęcia transakcji elektronicznych i możliwości twierdzenia przez użytkowników bankowości elektronicznej, że transakcje zostały oszukańczo zmienione.

Rozwiązanie tych zwiększonych problemów wymaga podjęcia przez banki rozsądnych działań, odpowiadających poziomowi istotności i rodzajowi transakcji bankowości elektronicznej, które zapewnią, że:

- systemy bankowości elektronicznej są zaprojektowane w sposób zmniejszający prawdopodobieństwo zainicjowania przez upoważnionych użytkowników niezamierzonych transakcji oraz umożliwiający klientom pełne zrozumienie ryzyk związanych z każdą zainicjowaną przez nich transakcją,
- tożsamość wszystkich stron transakcji jest potwierdzana, a także zachowywana jest kontrola nad potwierdzonym kanałem,
- dane o transakcjach finansowych są chronione przez zmianą, a wszelkie dokonane zmiany są wykrywalne.

Organizacje bankowe zaczęły stosować różne techniki, które pomagają uniemożliwić negowanie dokonanych transakcji i zapewniają poufność i rzetelność transakcji bankowości elektronicznej, takie jak certyfikaty depozytowe wykorzystujące publiczne klucze dostępu do infrastruktury (PKI).[26] Bank może wydać klientowi lub kontrahentowi certyfikat cyfrowy umożliwiający ich unikalną identyfikację / potwierdzanie tożsamości i zmniejszyć ryzyko negowania dokonanych transakcji. Pomimo, że w niektórych krajach specjalne przepisy prawne zapewniają klientom prawo do negowania transakcji, w niektórych krajowych jurysdykcjach wprowadzono ustawodawstwo zapewniające prawną skuteczność podpisów elektronicznych. Jest prawdopodobne, że w miarę rozwoju technologii techniki takie zyskają szerszą akceptację w skali ogólnoświatowej.

Zasada 6: Banki powinny upewniać się, że posiadają odpowiednie środki służące promowaniu adekwatnego podziału obowiązków w zakresie systemów, baz danych i aplikacji bankowości elektronicznej

Podział obowiązków jest podstawowym wewnętrznym mechanizmem kontrolnym służącym redukcji ryzyka oszustw w procesach i systemach operacyjnych i zapewnieniu

[26] W publicznym kluczu dostępu do infrastruktury (PKI) każda strona posiada parę kluczy, z których jeden jest prywatny, a drugi publiczny. Klucz prywatny jest poufny, i może go używać tylko jedna osoba. Wszystkie strony używają klucza publicznego. Klucz prywatny generuje podpis elektroniczny na dokumencie, a pary kluczy są zaprojektowane w taki sposób, iż komunikat zapisany przy użyciu klucza prywatnego może być odczytany jedynie przy użyciu drugiego klucza. Bank może być swym organem certyfikującym (CA) lub polegać na innej godnej zaufania stronie trzeciej w celu powiązania osoby lub firmy z certyfikatem cyfrowym. Jednak, jeżeli bank ma polegać w procesie potwierdzania tożsamości na certyfikacie cyfrowym wydanym przez stronę trzecią, to powinien upewnić się, że CA wydając certyfikat, zastosował taki sam poziom potwierdzenia tożsamości jaki użyłby bank w celu potwierdzenia tożsamości klienta. Główną wadą systemu potwierdzania tożsamości PKI jest skomplikowany proces wdrożenia.

właściwego systemu upoważnień do dysponowania aktywami spółki, oraz ewidencji i bezpieczeństwa aktywów. Podział obowiązków ma zasadnicze znaczenie dla dokładności i rzetelności danych i jest stosowany w celu zapobieżenia popełnianiu oszustw przez osobę fizyczną. Przy adekwatnym podziale obowiązków, oszustwo może być popełnione jedynie w wyniku zmowy.

Usługi bankowości elektronicznej mogą wymagać modyfikacji sposobów ustalania i przestrzegania podziału obowiązków, ponieważ transakcje są zawierane za pośrednictwem systemów elektronicznych, w których tożsamość może być łatwiej zamaskowana lub sfałszowana. Ponadto, funkcje operacyjne i transakcyjne stały się w wielu przypadkach bardziej sprężone i zintegrowane w aplikacjach bankowości elektronicznej. Z tego względu należy dokonać analizy mechanizmów kontrolnych wymaganych tradycyjnie dla zachowania podziału obowiązków, a także odpowiednio je dostosować w celu zachowania odpowiedniego poziomu kontroli. Ponieważ dostęp do słabo zabezpieczonych baz danych poprzez sieci wewnętrzne lub zewnętrzne jest łatwiejszy, należy podkreślać ścisłe procedury autoryzacji i identyfikacji, bezpieczną i solidną architekturę bezpośrednich procesów przetwarzania i adekwatne ścieżki audytu.

Praktyki stosowane powszechnie w celu ustalenia i stosowania podziału obowiązków dotyczących bankowości elektronicznej obejmują co następuje:

- procesy i systemy transakcyjne powinny być zaprojektowane w taki sposób, żeby uniemożliwiały każdemu pojedynczemu pracownikowi / wynajętemu usługodawcy zainicjowanie, autoryzację i realizację transakcji,
- należy zachować podział na osoby inicjujące dane statyczne (w tym treść strony internetowej) i osoby odpowiedzialne za weryfikację rzetelności tych danych,
- należy testować systemy bankowości elektronicznej w celu upewnienia się, że nie można obejść podziału obowiązków,
- należy zachować podział na osoby opracowujące i osoby administrujące systemami bankowości elektronicznej.[27]

Zasada 7: Banki powinny upewniać się, że posiadają właściwe mechanizmy kontroli autoryzacji i uprawnień dostępu do systemów, baz danych i aplikacji bankowości elektronicznej

W celu zachowania podziału obowiązków banki muszą w rygorystyczny sposób kontrolować zagadnienia autoryzacji i uprawnień dostępu. Brak adekwatnych mechanizmów kontroli autoryzacji może umożliwić osobom zmianę ich tożsamości, obejście podziału obowiązków i uzyskanie dostępu do systemów, baz danych lub aplikacji bankowości elektronicznej, do którego nie są uprawnione.

Zasady autoryzacji i praw dostępu w systemach bankowości elektronicznej mogą być określone w sposób scentralizowany lub zdecentralizowany w ramach banku. Stosowne dane są zazwyczaj przechowywane w bazach danych. Z tego względu ochrona tych baz danych przed manipulacją lub korupcją ma podstawowe znaczenie dla efektywnej kontroli autoryzacji.

[27] Lub należy stosować inne mechanizmy kontrolne.

W Załączniku III przedstawiono szereg rzetelnych praktyk użytecznych w ustanowieniu właściwej kontroli autoryzacji i praw dostępu do systemów, baz danych i aplikacji bankowości elektronicznej.

Zasada 8: Banki powinny upewniać się, że posiadają odpowiednie środki służące ochronie integralności transakcji, zapisów i informacji bankowości elektronicznej

Integralność danych oznacza pewność, że informacje przesyłane i przechowywane nie są zmieniane bez autoryzacji. Niezachowanie integralności danych dotyczących transakcji, zapisów i informacji może narażać banki na straty finansowe, jak również na znaczne ryzyko prawne i ryzyko reputacji.

Bezpośredni charakter procesów bankowości elektronicznej może sprawiać, że błędy w programie lub oszustwa mogą być trudniejsze do wykrycia na etapie wstępnym. Z tego względu jest ważne, aby banki wprowadzały bezpośrednie przetwarzanie danych w sposób zapewniający bezpieczeństwo i rzetelność oraz integralność danych.

Ponieważ transakcje bankowości elektronicznej są realizowane za pośrednictwem publicznych sieci, narażone są na dodatkowe zagrożenia w postaci korupcji danych, oszustw i manipulowania zapisami. W związku z powyższym, banki powinny upewniać się, że posiadają odpowiednie środki służące ustaleniu dokładności, kompletności i wiarygodności transakcji bankowości elektronicznej, zapisów oraz informacji przekazywanych za pośrednictwem internetu, przechowywanych w wewnętrznych bazach danych banku lub przesyłanych / przechowywanych w imieniu banku przez usługodawców, będących stronami trzecimi.[28] Powszechnie stosowane praktyki służące zachowaniu integralności danych w środowisku bankowości elektronicznej obejmują m.in.:

- transakcje bankowości elektronicznej powinny być realizowane w sposób, który czyni je w ciągu całego procesu wysoce odpornymi na manipulację,
- zapisy bankowości elektronicznej powinny być przechowywane, udostępniane i modyfikowane w sposób, który czyni je wysoce odpornymi na manipulację,
- procesy realizowania transakcji bankowości elektronicznej i prowadzenia zapisów powinny być zaprojektowane w taki sposób, aby faktycznie uniemożliwiały oszukanie systemu wykrywania nieautoryzowanych zmian,
- w celu uchronienia się przed wszelkimi zmianami w systemie bankowości elektronicznej, które mogą - wskutek błędu lub w sposób niezamierzony - narazić mechanizmy kontrolne lub wiarygodność danych, należy stosować adekwatne regulacje dotyczące kontrolowania zmian, w tym procedury monitorowania i testowania,
- wszelkie przypadki manipulowania transakcjami lub danymi bankowości elektronicznej powinny być wykrywane przez funkcje przetwarzania, monitorowania i rachunkowości transakcji.

Zasada 9: Banki powinny upewniać się, że posiadają jasno określone ścieżki audytu w zakresie transakcji bankowości elektronicznej

[28] Banki powinny upewniać się, że systemy prowadzenia zapisów są zaprojektowane i zainstalowane w sposób umożliwiający odzyskanie danych, które były przedmiotem manipulacji lub sfałszowania.

Świadczenie usług finansowych za pośrednictwem internetu może utrudniać bankom stosowanie i egzekwowanie wewnętrznych mechanizmów kontrolnych i utrzymywanie jasno określonych ścieżek audytu, jeśli banki nie przyjmą odpowiednich środków w odniesieniu do środowiska bankowości elektronicznej. Wyzwaniem dla banków nie jest tylko zapewnienie efektywnej kontroli wewnętrznej w wysoko zautomatyzowanych środowiskach, lecz także zapewnienie niezależnego audytu mechanizmów kontrolnych, szczególnie jeśli dotyczą one najważniejszych zdarzeń i aplikacji bankowości elektronicznej.

Może wystąpić osłabienie środowiska wewnętrznej kontroli, jeśli bank nie jest w stanie zachować jasno określonych ścieżek audytu w odniesieniu do prowadzonej przez siebie elektronicznej działalności bankowej. Dzieje się tak ponieważ większość, o ile nie wszystkie, posiadane dane i dowody mają postać elektroniczną. Dokonując ustaleń, w jakich obszarach należy zachować jasno określone ścieżki audytu, należy rozważyć następujące rodzaje transakcji bankowości elektronicznej:

- otwieranie, modyfikację lub zamykanie rachunku klienta,
- wszelkie transakcje mające konsekwencje finansowe,
- wszelkie udzielone klientowi upoważnienia do przekroczenia limitu,
- wszelkie przypadki udzielenia, modyfikacji lub cofnięcia praw lub przywilejów dostępu do systemów.

W Załączniku IV przedstawiono kilka rzetelnych praktyk pomocnych w zapewnieniu jasno określonych ścieżek audytu w odniesieniu do transakcji bankowości elektronicznej.

Zasada 10: Banki powinny podejmować odpowiednie kroki w celu zachowania poufności podstawowych informacji bankowości elektronicznej. Środki podejmowane w celu zachowania poufności powinny odpowiadać wrażliwości przekazywanych informacji i/lub informacji przechowywanych w bazach danych

Poufność oznacza zapewnienie, że podstawowe informacje pozostaną prywatnymi informacjami banku oraz, że osoby nieupoważnione nie mają do nich wglądu, ani nie mogą z nich korzystać. Nadużywanie lub nieautoryzowane ujawnienie danych naraża bank na ryzyko prawne i ryzyko reputacji. Powstanie bankowości elektronicznej stwarza dodatkowe wyzwania dla banków, ponieważ zwiększa ryzyko, że informacje przekazywane za pośrednictwem publicznej sieci lub przechowywane w bazach danych staną się dostępne dla nieupoważnionych lub niewłaściwych stron, a także ryzyko ich wykorzystania w sposób niezgodny z intencją klienta udzielającego informacji. Ponadto, zwiększone korzystanie z usługodawców może umożliwiać dostęp innych stron do kluczowych danych banku.

W celu sprostania wyzwaniom w zakresie zachowania poufności kluczowych informacji bankowości elektronicznej, banki muszą upewnić się, czy:

- dostęp do wszystkich poufnych danych i zapisów banku posiadają wyłącznie odpowiednio upoważnione i potwierdzone osoby, agenci lub systemy,
- wszystkie poufne dane banku są przechowywane w bezpieczny sposób i chronione przed nieautoryzowanym wglądem lub modyfikacją podczas transmisji za pośrednictwem publicznych, prywatnych lub wewnętrznych sieci,

- w sytuacji, gdy strony trzecie mają dostęp do danych poprzez relacje związane ze zlecaniem usług na zewnątrz, należy przestrzegać stosowanych przez bank standardów i mechanizmów kontroli wykorzystania i ochrony danych,
- każdy dostęp do danych zastrzeżonych wymaga zalogowania, a bank podejmuje odpowiednie działania w celu uniemożliwienia manipulacji loginami dostępu.

C. Zarządzanie ryzykiem prawnym i ryzykiem reputacji (Zasady od 11 do 14)

Szczególne regulacje i ustawy dotyczące ochrony klienta i poufności danych różnią się w poszczególnych jurysdykcjach. Generalnie jednak banki są wyraźnie zobowiązane do zapewnienia swoim klientom komfortu w zakresie ujawniania danych, ochrony danych o klientach i dostępności usług na poziomie zbliżonym do zapewnianego w przypadku transakcji realizowanych za pośrednictwem tradycyjnych bankowych kanałów dystrybucji.

Zasada 11: Banki powinny udostępniać odpowiednie informacje na swych stronach internetowych, które umożliwią ich potencjalnym klientom wyciągnięcie dobrze ugruntowanych wniosków na temat tożsamości banku oraz jego statusu prawnego przed rozpoczęciem realizacji transakcji bankowości elektronicznej

W celu minimalizacji ryzyka prawnego i ryzyka reputacji wiążącego się z elektroniczną działalnością bankową prowadzoną w kraju i zagranicą, banki powinny udostępniać odpowiednie informacje na swych stronach internetowych, które umożliwią klientom wyciągnięcie dobrze ugruntowanych wniosków na temat tożsamości banku i jego statusu prawnego przed rozpoczęciem realizacji transakcji bankowości elektronicznej.

Przykłady informacji, które bank może udostępnić na swej stronie internetowej obejmują:

- nazwę banku oraz miejsce lokalizacji jego siedziby (oraz placówek lokalnych, jeśli właściwe),
- informacje na temat głównej(-ych) instytucji nadzoru bankowego odpowiedzialnej(-ych) za nadzorowanie centrali banku,
- sposób kontaktowania się z centrum obsługi klientów banku w sprawach dotyczących problemów w zakresie usług, skarg, podejrzewanych przypadków nadużycia rachunków, etc.,
- sposób kontaktowania się i wykorzystania właściwego rzecznika do spraw ochrony konsumentów,
- sposobu zasięgania informacji na temat właściwych krajowych systemów rekompensowania lub gwarantowania depozytów, jak również wysokości zapewnianej przez nie gwarancji (lub zamieszczenie przejścia na strony internetowe, które zawierają takie informacje),
- inne stosowne informacje lub informacje wymagane w konkretnych jurysdykcjach.[29]

[29] Na przykład, bank może wymienić kraje, w których zamierza świadczyć usługi bankowości elektronicznej, bądź – przeciwnie - kraje, w których nie zamierza świadczyć takich usług.

Zasada 12: Banki powinny podejmować odpowiednie kroki w celu zapewnienia przestrzegania wymagań w zakresie ochrony danych o klientach obowiązujących w jurysdykcjach, w których bank oferuje produkty lub świadczy usługi bankowości elektronicznej

Zachowanie poufnego charakteru danych o kliencie jest podstawowym obowiązkiem banku. Niewłaściwe użycie lub ujawnienie poufnych danych o kliencie bez upoważnienia naraża bank zarówno na ryzyko prawne jak i ryzyko reputacji. W celu sprostania wyzwaniom w zakresie zachowania poufnego charakteru informacji o kliencie, banki powinny podejmować umiarkowane wysiłki w celu zapewnienia, że:

- stosowana przez bank polityka i standardy poufności danych o klientach są zgodne ze wszystkimi ustawami i regulacjami obowiązującymi w jurysdykcjach, w których bank oferuje produkty lub świadczy usługi bankowości elektronicznej,
- klienci posiadają znajomość regulacji banku dotyczących ochrony danych oraz związanych z nimi zagadnień poufności w zakresie produktów i usług bankowości elektronicznej,
- klienci mają możliwość nie wyrażenia zgody na przekazywanie przez bank osobom trzecim dla celów wzajemnego marketingu wszelkich informacji dotyczących ich potrzeb osobistych, interesów, pozycji finansowej i korzystania z usług bankowych,
- dane o klientach nie są wykorzystywane dla celów niezgodnych z przeznaczeniem lub dla celów nie wynikających z upoważnień udzielonych przez klientów,[30]
- strony trzecie posiadające dostęp do danych o klientach w wyniku realizacji umów o zlecanie usług są zobowiązane do przestrzegania standardów banku w zakresie tych danych.

W Załączniku V przedstawiono kilka rzetelnych praktyk pomocnych w zachowaniu poufności danych o klientach korzystających z bankowości elektronicznej.

Zasada 13: Banki powinny posiadać zdolność efektywnego świadczenia usług, zapewniać ciągłość działalności oraz posiadać procesy planowania awaryjnego w celu zapewnienia dostępności systemów i usług bankowości elektronicznej

W związku z koniecznością zabezpieczenia banków przed ryzykiem gospodarczym, prawnym i ryzykiem reputacji, usługi bankowości elektronicznej muszą być świadczone w sposób i w czasie zgodnym z oczekiwaniami klientów. Osiągnięcie tego celu wymaga zdolności banku do dostarczania usług bankowości elektronicznej użytkownikom końcowym ze źródeł podstawowych (np. wewnętrzne systemy lub aplikacje banku) lub wtórnych.(np. systemy lub aplikacje usługodawców). Utrzymanie adekwatnego poziomu dostępności usług zależy także od zdolności awaryjnych systemów podtrzymywania do redukcji zagrożeń wynikających z ataków wiążących się z blokowaniem usług, bądź z innych zdarzeń, które mogą spowodować zakłócenia prowadzonej działalności.

Wyzwania dla zachowania ciągłej dostępności systemów i aplikacji bankowości elektronicznej mogą być poważne biorąc pod uwagę możliwość wystąpienia dużego popytu na transakcje, szczególnie w godzinach szczytu. Ponadto, znaczenie dużej zdolności świadczenia

[30] W niektórych jurysdykcjach ustawy i regulacje nie zobowiązują banków do uzyskania zezwolenia klienta na wykorzystywanie danych o nim dla celów wewnętrznych. Mogą jednak zobowiązywać banki do zapewnienia klientowi możliwości sprzeciwu wobec przekazywania takich informacji przez bank osobie trzeciej lub podmiotowi zależnemu. W innych jurysdykcjach klienci mogą mieć prawo do uniemożliwienia bankowi wykorzystywania danych o klientach dla celów wewnętrznych lub zewnętrznych.

usług, ciągłości działalności i planowania awaryjnego zwiększają duże oczekiwania klientów dotyczące krótkiego cyklu przetwarzania transakcji ich stałej dostępności (24 godziny x 7 dni). W celu zapewnienia klientom zgodnej z ich oczekiwaniami dostępności usług bankowości elektronicznej, banki muszą zapewnić, że:

- bieżąca pojemność systemu bankowości elektronicznej i jego przyszłe możliwości zostały zanalizowana w świetle ogólnej dynamiki rynku elektronicznej działalności handlowej i przewidywanego poziomu akceptacji produktów i usług bankowości elektronicznej przez klientów,[31]
- dokonuje się oszacowań, testowania awaryjnego i okresowych analiz zdolności przetwarzania transakcji bankowości elektronicznej,
- istnieją odpowiednie plany dotyczące ciągłości działalności podstawowych systemów przetwarzania i dostarczania usług bankowości elektronicznej i plany awaryjne, plany te są poddawane okresowym testom.

W Załączniku VI przedstawiono kilka rzetelnych praktyk w zakresie zdolności efektywnego świadczenia usług, zapewnienia ciągłości działalności oraz planowania awaryjnego.

Zasada 14: Banki powinny opracować odpowiednie plany reagowania na incydenty służące zarządzaniu, przeciwdziałaniu i minimalizacji problemów wynikających z nieoczekiwanych zdarzeń, w tym ataków wewnętrznych i zewnętrznych, które mogą szkodzić funkcjonowaniu systemów i świadczeniu usług bankowości elektronicznej

Efektywne mechanizmy reagowania na incydenty mają podstawowe znaczenie dla minimalizowania ryzyka operacyjnego, prawnego, i ryzyka reputacji, które są skutkiem nieoczekiwanych zdarzeń, takich jak ataki wewnętrzne i zewnętrzne, i mogą wpływać na funkcjonowanie systemów i świadczenie usług bankowości elektronicznej. Banki powinny opracowywać odpowiednie plany reagowania na incydenty, w tym strategie komunikowania się, które zapewniają ciągłość prowadzonej działalności, kontrolę ryzyka reputacji i ograniczają zobowiązania związane z zakłóceniami świadczonych przez banki usług bankowości elektronicznej, w tym z zakłóceniami funkcjonowania systemów i usług zleconych na zewnątrz.

W celu zapewnienia efektywnego reagowania na nieprzewidziane incydenty, banki powinny opracować:

- Plany reagowania na incydenty uwzględniające przywracanie systemów i usług w różnych scenariuszach, różnej działalności i lokalizacjach geograficznych. Analizy scenariuszy powinny uwzględniać kwestię prawdopodobieństwa wystąpienia ryzyka oraz jego wpływ na bank. Systemy bankowości elektronicznej zlecone usługodawcom będącym stronami trzecimi powinny stanowić integralną część tych planów.
- Mechanizmy służące niezwłocznemu wykrywaniu incydentu lub sytuacji kryzysowej, oceny ich istotności oraz kontrolowaniu ryzyka reputacji związanego z zakłóceniami usług.[32]

---

[31] Należy prowadzić ciągłą analizę bieżącej i przyszłej pojemności podstawowych systemów dostawczych bankowości elektronicznej.

[32] Monitorowanie stanowiska udzielającego pomocy klientom i działań dotyczących obsługi klientów oraz regularna analiza skarg klientów mogą być pomocne w ustaleniu luk pomiędzy informacjami wykrytymi i zgłoszonymi za pośrednictwem ustalonych mechanizmów kontroli bezpieczeństwa, a faktycznymi nieuprawnionymi działaniami.

- Strategię komunikacji w adekwatny sposób uwzględniającą kwestie kontaktu z rynkiem zewnętrznym i mediami w przypadku naruszenia bezpieczeństwa, ataków sieciowych i/lub awarii systemów bankowości elektronicznej.
- Jasno określony proces alarmowania właściwych władz nadzorczych w przypadkach wystąpienia istotnego naruszenia bezpieczeństwa lub zakłóceń działalności.
- Powołać zespoły ds. reagowania na incydenty dysponujące uprawnieniami umożliwiającymi podejmowanie działań w nagłych okolicznościach, przeszkolone w zakresie analizy wykrywania incydentów / systemów reagowania oraz interpretowania znaczenia ich skutków.
- Jasno określony system podległości obejmujący zarówno operacje wewnętrzne jak i zlecone, zapewniający podejmowanie natychmiastowych działań odpowiadających powadze incydentu. Ponadto, należy opracować procedury dotyczące powiadamiania i komunikacji wewnętrznej, które, jeśli właściwe, powinny obejmować informowanie Rady.
- Proces zapewniający właściwy tryb i czas informowania odpowiednich stron zewnętrznych, w tym klientów banku, kontrahentów i media, o rozwoju wydarzeń w zakresie istotnych przypadków zakłóceń bankowości elektronicznej oraz o wznawianiu tej działalności.
- Proces gromadzenia i zabezpieczania dowodów sądowych, umożliwiających odpowiednie późniejsze analizy wszelkich incydentów dotyczących bankowości elektronicznej, jak również pomagających w ściganiu osób odpowiedzialnych za ataki.

Załącznik I: Rzetelne praktyki kontroli bezpieczeństwa w bankowości elektronicznej

1. Należy tworzyć i utrzymywać profile bezpieczeństwa. Dotyczy to także konkretnych przywilejów autoryzacji przyznawanych wszystkim użytkownikom systemów i aplikacji, w tym wszystkim klientom, wewnętrznym użytkownikom bankowym oraz usługodawcom, którym zlecono usługi. W celu wsparcia właściwego podziału obowiązków należy opracować także mechanizmy kontroli dostępu elektronicznego.[33]

2. Dane i systemy bankowości elektronicznej powinny być klasyfikowane zgodnie z ich wrażliwością i znaczeniem oraz odpowiednio chronione. W celu ochrony wszystkich wrażliwych systemów bankowości elektronicznej i systemów wysokiego ryzyka, serwerów, baz danych i aplikacji należy stosować odpowiednie mechanizmy, takie jak szyfrowanie, kontrola dostępu i plany odzyskiwania danych.

3. Przechowywanie danych wrażliwych lub danych wysokiego ryzyka w systemach komputerów biurowych lub komputerów przenośnych organizacji powinno być ograniczone do minimum i właściwie chronione poprzez szyfrowanie, kontrolę dostępu i plany odzyskiwania danych.

4. W celu zapobieżenia dostępowi do podstawowych systemów, serwerów, baz danych i aplikacji bankowości elektronicznej bez upoważnienia[34] należy wprowadzić odpowiednie mechanizmy kontroli fizycznego dostępu.

5. Należy stosować odpowiednie techniki służące redukcji zewnętrznych zagrożeń dla systemów bankowości elektronicznej, w tym korzystać z:

   - oprogramowania wykrywającego wirusy we wszystkich najważniejszych punktach wejścia (np. w serwerach o zdalnym dostępnie, serwerach obsługujących pocztę elektroniczną) i w każdym systemie komputerów biurowych.
   - oprogramowania wykrywającego próby włamań do systemu oraz z innych narzędzi oceny bezpieczeństwa służących okresowemu badaniu sieci, serwerów i stosowanych rozgraniczeń w celu wykrycia słabości i/lub przypadków naruszenia procedur bezpieczeństwa i mechanizmów kontrolnych.
   - testowania pod kątem penetracji sieci wewnętrznych i zewnętrznych.

6. Należy stosować rygorystyczny proces analizy bezpieczeństwa wobec wszystkich pracowników i usługodawców zajmujących wrażliwe stanowiska.

---

[33] Definicje bezpieczeństwa i standardów jakościowych oraz stopień polegania na systemach certyfikacji mogą dotyczyć konkretnych instytucji lub stanowić standard (tzn. w ramach krajowego systemu bankowego, w celu zwiększenia i kształtowania poziomu bezpieczeństwa elektronicznej działalności bankowej). Banki mogą się także zdecydować na ustanowienie scentralizowanego lub zdecentralizowanego systemu praw dostępu. Na przykład, może istnieć tylko jedna jednostka autoryzująca, odpowiedzialna za przyznawanie praw dostępu konkretnym osobom, grupom lub funkcjom w ramach banku. Może też istnieć szereg jednostek autoryzujących, realizujących różne potrzeby w ramach różnych pionów organizacyjnych.

[34] Powinno to obejmować mechanizmy kontrolne zabezpieczające przed nieupoważnionym dostępem do systemów stron zewnętrznych, takich jak goście, zleceniobiorcy i technicy. Strony te mogą mieć dostęp do pomieszczeń, chociaż mogą nie być bezpośrednio zaangażowane w usługi bankowości elektronicznej.

Załącznik II: Rzetelne praktyki zarządzania zleconymi systemami i usługami bankowości elektronicznej

1. Banki powinny przyjmować odpowiednie procesy oceny decyzji w sprawie zlecania na zewnątrz systemów i usług bankowości elektronicznej.

   - Kierownictwo banku powinno w jasny sposób ustalić cele strategiczne, korzyści i koszty zawiązane z zawieraniem umów o zlecanie usług z zakresu bankowości elektronicznej ze stronami trzecimi.
   - Decyzja w sprawie zlecenia podstawowej funkcji lub usługi bankowości elektronicznej powinna być zgodna ze strategią gospodarczą banku, oparta na jasno zidentyfikowanej potrzebie gospodarczej i określać szczególne ryzyka wynikające ze zlecenia.
   - Wszystkie obszary banku, których to dotyczy, muszą rozumieć w jaki sposób dostawca(-y) usługi będzie(-ą) wspierał(-li) strategię banku w zakresie bankowości elektronicznej i jakie miejsce zajmuje(-ą) w strukturze operacyjnej tej działalności.

2. Przed wyborem dostawcy usług bankowości elektronicznej oraz z odpowiednią częstotliwością po dokonaniu wyboru, banki powinny prowadzić odpowiednią analizę ryzyka i ocenę należytej staranności.

   - Banki powinny rozważyć opracowanie procesu występowania o propozycje ze strony szeregu dostawców usług bankowości elektronicznej i kryteria wyboru spomiędzy różnych propozycji.
   - Po ustaleniu potencjalnego dostawcy usług, bank powinien przeprowadzić odpowiednią analizę należytej staranności, w tym analizę ryzyka wiążącego się z siłą finansową dostawcy usług, jego reputacją, polityką i kontrolą zarządzania ryzykiem oraz zdolnością do wykonania swych zobowiązań.
   - Następnie, banki powinny regularnie monitorować i, jeśli właściwe,[35] prowadzić analizę należytej staranności w zakresie zdolności dostawcy usług do wypełniania spoczywających na nim zobowiązań dotyczących usług oraz zarządzania związanym z tymi usługami ryzykiem przez cały okres obowiązywania umowy.
   - Banki muszą upewniać się, że poświęcają adekwatne zasoby kontrolowaniu umów dotyczących usług wspierających bankowość elektroniczną.
   - Należy w jasny sposób przydzielić obowiązki dotyczące kontroli umów zlecania usług bankowości elektronicznej.
   - Należy opracować odpowiednią strategię zarządzania ryzykiem w przypadku konieczności wypowiedzenia umowy o zlecenie usług.

3. Banki powinny przyjmować odpowiednie procedury zapewniania adekwatności umów regulujących bankowość elektroniczną. Umowy regulujące zlecone działania z zakresu

[35] Zasięg ciągłej analizy należytej staranności powinien zależeć od poziomu istotności zleconych operacji i stopnia zmian w czasie systemów bankowości elektronicznej lub zarządzania ryzykiem, w tym od przypadków wszelkiego ewentualnego zlecania usług podwykonawcom przez dostawcę usług.

bankowości elektronicznej powinny przykładowo uwzględniać następujące zagadnienia:[36]

- Należy jasno określić zobowiązania umowne poszczególnych stron, jak również odpowiedzialność za podejmowanie decyzji, w tym decyzji dotyczących zlecania ważnych usług podwykonawcom.

- Należy jasno określić obowiązki informacyjne względem dostawcy usług oraz obowiązki informacyjne dostawcy usług względem banku. Informacje przekazywane przez dostawcę usług powinny być na tyle aktualne i wszechstronne, aby umożliwiać bankowi dokonanie adekwatnej oceny poziomu usług i ryzyka. Umowa winna formułować progi istotności i procedury stosowane w celu poinformowania banku o zakłóceniach usług, przypadkach naruszenia bezpieczeństwa i innych zdarzeniach stanowiących znaczne ryzyko dla banku.

- Należy jasno sformułować postanowienia dotyczące konkretnie zagadnień zakresu informacji, własności danych przechowywanych na serwerach i w bazach danych dostawcy usług oraz prawo banku do odzyskania tych danych w związku z wygaśnięciem lub wypowiedzeniem umowy.

- Należy określić oczekiwania dotyczące funkcjonowania w warunkach normalnych i w warunkach skrajnych.

- Należy określić adekwatne środki i gwarancje, np. poprzez wprowadzenie klauzul dotyczących audytu, zapewniające zgodność dostawcy usług z polityką banku.

- Należy zawrzeć porozumienia dotyczące podejmowania odpowiednich w czasie i uporządkowanych interwencji oraz działań naprawczych w przypadku niezadowalającej realizacji obowiązków przez dostawcę usług.

- W przypadku transgranicznych umów zlecania usług ustalić, którego kraju ustawy i regulacje, w tym dotyczące prywatności danych i innego rodzaju ochrony klientów, mają zastosowanie.

- Umowa winna jasno określać prawo banku do prowadzenia niezależnych badań i/lub audytów w zakresie bezpieczeństwa, kontroli wewnętrznej i planów skrajnych warunków.

4. Banki powinny upewniać się, że prowadzone są okresowe niezależne audyty wewnętrzne i/lub zewnętrzne zleconych operacji w co najmniej takim samym zakresie jaki byłby stosowany w przypadku prowadzenia operacji na miejscu.[37]

---

[36] Podobnie jak w przypadku innych umów, które może zawrzeć bank, jego doradca prawny lub departament prawny powinien dokonać analizy wszystkich warunków umów regulujących kwestie zlecania usług bankowości elektronicznej.

[37] Banki nie posiadające konkretnej funkcji audytu wewnętrznego powinny, jako minimum, zapewniać, aby analiz efektywności zarządzania umowami w sprawie zlecania usług nie prowadzili pracownicy zaangażowani w zarządzanie umowami o zlecanie usług.

- W przypadku umów dotyczących zlecania na zewnątrz podstawowych lub technologicznie zaawansowanych usług / aplikacji bankowości elektronicznej, banki mogą zapewnić wykonywanie innych okresowych badań przez niezależne strony trzecie dysponujące dostateczną ekspertyzą techniczną.

5. Banki powinny opracowywać odpowiednie plany awaryjne dotyczące zleconych działań z zakresu bankowości elektronicznej.

   - Banki muszą opracowywać i okresowo testować swe plany awaryjne dotyczące wszystkich podstawowych systemów i usług bankowości elektronicznej, które zostały zlecone stronom trzecim.

   - W celu zapewnienia ciągłości usług bankowości elektronicznej w przypadku zakłóceń dotyczących zleconych operacji, plany awaryjne powinny uwzględniać wiarygodne najgorsze scenariusze.

   - Banki powinny powołać zespół odpowiedzialny za zarządzanie działaniami naprawczymi i ocenę finansowego wpływu zakłóceń w zleconych usługach bankowości elektronicznej.

6. Banki świadczące usługi bankowości elektronicznej na rzecz stron trzecich powinny upewniać się, że ich operacje, obowiązki i zobowiązania są wystarczająco jasne, aby obsługiwane instytucje mogły w adekwatny sposób dokonywać własnych efektywnych analiz należytej staranności i prowadzić ciągłą kontrolę realizacji umów.

   - Banki zobowiązane są udzielać obsługiwanym instytucjom informacji niezbędnych do identyfikacji, kontroli i monitorowania wszelkich ryzyk związanych z realizacją umów dotyczących usług bankowości elektronicznej.

Załącznik III: Rzetelne praktyki autoryzacji dostępu do aplikacji bankowości elektronicznej

1. Wszystkim osobom, agentom lub systemom, które prowadzą elektroniczną działalność bankową, należy przypisać konkretne przywileje autoryzacji i dostępu.

2. Wszystkie systemy bankowości elektronicznej powinny być skonstruowane w taki sposób, aby zapewniały ich interakcję z ważną bazą danych dotyczących autoryzacji.

3. Żaden indywidualny agent lub system nie powinien być uprawniony do zmiany swych własnych uprawnień lub przywilejów dostępu w bazie danych dotyczących autoryzacji dostępu do bankowości elektronicznej.[38]

4. W każdym przypadku nadanie nowej osobie, agentowi lub systemowi przywilejów dostępu lub ich zmiana w bazie danych dotyczących autoryzacji dostępu do bankowości elektronicznej powinno być we właściwy sposób autoryzowane przez uwiarygodnione źródło wyposażone w odpowiednie uprawnienia i podlegające odpowiedniej i bieżącej kontroli oraz ścieżkom audytu.

5. Należy wprowadzić odpowiednie kroki służące uodpornieniu baz danych dotyczących autoryzacji dostępu do bankowości elektronicznej na manipulacje. Wszelkie przypadki manipulacji powinny być wykrywalne poprzez procesy ciągłego monitorowania. Konieczność dokumentowania takich prób manipulacji wymaga istnienia dostatecznych ścieżek audytu.

6. Baza danych dotyczących autoryzacji dostępu do bankowości elektronicznej, która została poddana manipulacji, nie powinna być używana do czasu jej zastąpienia przez sprawdzoną bazę danych.

7. Należy wprowadzić mechanizmy kontrolne zapobiegające zmianom poziomów autoryzacji podczas sesji transakcji bankowości elektronicznej, a wszelkie próby zmiany autoryzacji powinny być rejestrowane i poddawane uwadze kierownictwa

[38] Ponieważ zasada ta może być niewykonalna w przypadku użytkowników będących administratorami systemu, należy wprowadzić, w celu monitorowania działalności tych użytkowników rachunków, inne surowe wewnętrzne mechanizmy kontrolne i podział obowiązków.

Załącznik IV: Rzetelne praktyki w zakresie ścieżek audytu w systemach bankowości elektronicznej

1. Wszystkie transakcje bankowości elektronicznej należy w odpowiedni sposób rejestrować w celu ustanowienia jasno określonej ścieżki audytu oraz pomocy w rozwiązywaniu sporów.

2. Systemy bankowości elektronicznej powinny być zaprojektowane i zainstalowane w sposób umożliwiający wychwycenie i zabezpieczenie dowodów sądowych. Zabezpieczenie oznacza adekwatną kontrolę dowodów, a także zapobieganie manipulacjom oraz gromadzeniu fałszywych dowodów.

3. W przypadkach, gdy za systemy przetwarzania danych i związane z nimi ścieżki audytu odpowiada usługodawca będący stroną trzecią:

   - bank powinien upewniać się, że posiada dostęp do odpowiednich ścieżek audytu utrzymywanych przez usługodawcę,

   - oraz, że ścieżki audytu utrzymywane przez usługodawcę spełniają standardy banku.

Załącznik V: Rzetelne praktyki pomocne w zachowaniu poufności informacji o klientach bankowości elektronicznej

1. Banki powinny używać odpowiednich technik kryptograficznych, szczególnych protokołów lub innych mechanizmów kontroli bezpieczeństwa, zapewniających poufność danych o klientach bankowości elektronicznej.

2. Banki powinny opracować odpowiednie procedury i mechanizmy kontrolne w celu okresowej oceny swej infrastruktury i protokołów bankowości elektronicznej w zakresie bezpieczeństwa klientów.

3. Banki powinny upewniać się, że realizowana przez współpracujących z nimi dostawców usług będących stronami trzecimi polityka w zakresie poufności i prywatności informacji jest spójna z polityką banków.

4. Banki powinny podejmować odpowiednie kroki w celu poinformowania klientów bankowości elektronicznej o zasadach poufności i prywatności stosowanych wobec informacji na ich temat. Kroki te mogą obejmować:

   - Informowanie klientów na temat polityki banku w sprawie poufności danych, ewentualnie na stronie internetowej banku. Podstawowe znaczenie dla zapewnienia pełnego zrozumienia polityki poufności przez klienta ma stosowanie jasnego i zwięzłego języka. Jest prawdopodobne, że większość klientów nie przeczyta długich, choć precyzyjnych, opisów prawnych.

   - Instruowanie klientów na temat potrzeby ochrony ich haseł, osobistych numerów identyfikacyjnych (PIN) oraz innych danych bankowych i/lub osobowych.

   - Dostarczanie klientom informacji dotyczących ogólnego bezpieczeństwa ich komputera osobistego, w tym korzyści płynących ze stosowania oprogramowania antywirusowego, mechanizmów kontroli fizycznego dostępu i osobistych rozgraniczeń od statycznych połączeń internetowych.

Załącznik VI: Rzetelne praktyki w zakresie zdolności świadczenia usług, ciągłości działania i planów awaryjnych dotyczących bankowości elektronicznej

1. Wszystkie usługi i aplikacje bankowości elektronicznej, w tym dostarczane przez usługodawców będących stronami trzecimi, należy identyfikować i oceniać pod względem ich znaczenia.

2. Należy dokonywać oceny ryzyka w odniesieniu do każdej podstawowej usługi i aplikacji bankowości internetowej, w tym oceny potencjalnego wpływu wszelkich zakłóceń działalności na ryzyko kredytowe banku oraz jego ryzyko rynkowe, płynności, prawne, operacyjne i ryzyko reputacji.

3. Należy ustanowić kryteria funkcjonowania dla każdej podstawowej usługi i aplikacji bankowości elektronicznej. Poziom usług powinien być monitorowany pod kątem takich kryteriów. Należy podejmować odpowiednie środki w celu zapewnienia, że systemy bankowości elektronicznej mogą obsłużyć dużą i małą liczbę transakcji oraz, że funkcjonowanie i pojemność systemów są zgodne z oczekiwaniami banku w zakresie przyszłego rozwoju bankowości elektronicznej.

4. Należy rozważyć opracowanie alternatywnych rozwiązań przetwarzania danych, aby sprostać popytowi, gdy systemy bankowości elektronicznej osiągną określone pułapy zdolności przetwarzania.

5. Należy sformułować plany ciągłości bankowości elektronicznej uwzględniające wszelkie uzależnienia od dostawców usług będących stronami trzecimi oraz wszelkie inne zewnętrzne uzależnienia wymagane dla przywrócenia działalności.

6. Plany awaryjne dotyczące bankowości elektronicznej powinny określić proces przywracania lub zastępowania zdolności przetwarzania bankowości elektronicznej, rekonstrukcji informacji wspierających transakcje i obejmować, podejmowane w przypadku zakłócenia działalności, środki służące wznowieniu dostępności podstawowych systemów i aplikacji bankowości elektronicznej.

Grupa ds. Bankowości Elektronicznej Bazylejskiego Komitetu ds. Nadzoru Bankowego
Przewodniczący:
Pan John Hawke Jr. – Kontroler Waluty, Waszyngton DC

Członkowie:

Commission Bancaire et Financière, Belgia	Pan Jos Meuleman Pan Koen Algoet
Urząd Superintendenta ds. Instytucji Finansowych, Kanada	Pani Judy Cameron Pan Brad Sullivan
Commission Bancaire, Francja	Pan Alain Duchâteau Pan Jerôme Deslandes
Bundesaufsichtsamt für das Kreditwesen, Niemcy	Pan Stefan Czekay
Deutsche Bundesbank, Niemcy	Pani Magdalene Heid Pan Andi Kloefer
Banca d'Italia, Włochy	Pan Filippo Siracusano
Agencja Nadzoru Finansowego, Japonia	Pan Kazuo Kojima Pan Tadaaki Kawamura
Bank Japonii, Japonia	Pan Toshihiko Mori Pan Hiroaki Kuwahara Pani Tomoko Suzuki
Commission de Surveillance du Secteur Financier, Luxembourg	Pan David Hagen Pan Claude Bernard
De Nederlandsche Bank N.V., Holandia	Pan Erik Smid
Banco de España, Hiszpania	Pani Maria Jesús Nieto
Organ Nadzoru Finansowego, Szwecja	Pan Jan Hedqvist
Federalna Komisja Bankowa, Szwajcaria	Pan Daniel Schmid
Financial Services Authority, Wielka Brytania	Pan Jeremy Quick Pani Katy Martin
Urząd Kontrolera Waluty (OCC), Stany Zjednoczone	Pan Hugh Kelly Pan Clifford Wilke
Rada Gubernatorów Systemu Rezerwy Federalnej, Stany Zjednoczone	Pani Heidi Richards Pan Jeff Marquardt
Federalna Korporacja Ubezpieczenia Depozytów, Stany Zjednoczone	Pani Sandra Thomson Pan John Carter
Bank Rezerwy Federalnej Nowego Jorku, Stany Zjednoczone	Pan George Juncker Pani Barbara Yelcich Pan Christopher Calabia Pan Thomas Whitford
Sekretariat, Bazylejski Komitet ds. Nadzoru Bankowego, Bank Rozrachunków Międzynarodowych	Pan J-P Svoronos

Obserwatorzy:

Australijskie Władze ds. Regulacji Ostrożnościowych:	Pan Graham Johnson
Europejski Bank Centralny:	Pan Michael Olsen
Władze Monetarne Hong Kongu:	Pan Brian Lee
Władze Monetarne Singapuru:	Pan Enoch Ch'ng