Strategia i procesy zarządzania ryzykiem operacyjnym

Ryzyko operacyjne to możliwość wystąpienia straty wynikającej z niedostosowania lub zawodności procesów wewnętrznych systemów , ludzi oraz zdarzeń zewnętrznych.

Podstawy funkcjonowania systemu zarzadzania ryzykiem operacyjnym wyznaczają „ Zasady zarzadzania ryzykiem operacyjnym w Banku Spółdzielczym w Łukowie.

Celem zarządzania ryzykiem operacyjnym w Banku jest zapewnienie bezpiecznego przebiegu wszystkich procesów biznesowych w Banku poprzez:

1. Identyfikację ryzyka operacyjnego w określonych obszarach działania Banku.
2. Utworzenie bazy danych w celu gromadzenia informacji o zdarzeniach ryzyka operacyjnego i stratach powstających w wyniku zakłóceń w działalności Banku.
3. Monitorowanie i raportowanie incydentów o których mowa w pkt 2.
4. Tworzenie mapy ryzyka w celu określenia działań zmierzających do zmniejszenia skutków ryzyka operacyjnego.
5. Wykorzystanie mapy ryzyka operacyjnego w opracowaniu „Polityki zarządzania ryzykiem operacyjnym" (zawierającej min. plan nakładów inwestycyjnych), „Polityki kadrowej" itp., stanowiących element założeń do planu finansowego.
6. Kontrolę i ocenę procesu zarządzania ryzykiem operacyjnym w Banku.
7. Ograniczanie skutków ryzyka operacyjnego.
8. Gromadzenie informacji o zdarzeniach ryzyka operacyjnego mających miejsce w najbliższym otoczeniu Banku oraz w miarę możliwości o sposobach porycia strat ww. zdarzeń i podjętych działaniach mitygujących.

Zgodnie z „Rekomendacją M" wydaną przez Komisję Nadzoru Finansowego czynnikami ryzyka operacyjnego są:

1. Zasoby ludzkie i warunki pracy.
2. Procesy i systemy - integralność procesów biznesowych oraz systemów informatycznych i technicznych.
3. Bezpieczeństwo:
   1) informatyczne i teleinformatyczne, zasady zarządzania ryzykiem w zakresie bezpieczeństwa środowiska teleinformatycznego i informacji zawiera rozdział 10 niniejszej Instrukcji;
   2) informacji prawnie chronionej;
   3) alternatywnych kanałów dostępu do usług i informacji bankowych (np. bankomaty, internet);
   4) fizyczne;
   5) związane z zasobami ludzkimi;
   6) klientów - zmiany w środowisku biznesowym;
   7) produktów - wdrażanie nowych produktów;
4. Outsourcing - procesy zlecone na zewnątrz.
5. Przestępstwa.
6. Awarie, klęski, katastrofy.

Wystąpienie zdarzenia wynikającego z ryzyka operacyjnego oznacza dla Banku:

1. Możliwość wystąpienia strat finansowych.
2. Możliwość znacznego wzrostu kosztów funkcjonowania.
3. Możliwość wystąpienia strat niefinansowych takich jak:
   1) utrata klientów,
   2) skargi klientów, niezadowolenie,
   3) negatywne postrzeganie Banku,
   4) utrata wiarygodności Banku jako instytucji zaufania publicznego.
4. Wzrost innych rodzajów ryzyka na skutek zdarzeń z tzw. pogranicza ryzyk. Przykładem zdarzenia z pogranicza ryzyka jest wyłudzenie kredytu, które jest ujmowane zarówno w ocenie ryzyka kredytowego jak i w ocenie ryzyka operacyjnego (oszustwo).

Ocena ryzyka przeprowadzana jest na podstawie danych zebranych w procesie identyfikacji i oceny zdarzeń operacyjnych z wszystkich komórek organizacyjnych Banku oraz po dokonaniu analizy i oceny tych danych przez Komórkę monitorująca ryzyko min. w następującym zakresie:

1. Struktury ryzyka (rodzaj zaistniałych zdarzeń, czynniki generujące ryzyko).
2. Obszarów powstawania zagrożeń (w procesach, w poszczególnych liniach biznesowych i innych zakresach działania Banku).
3. Skali zagrożeń i strat.
4. Poziomu ryzyka.
5. Tworzenia planów awaryjnych zachowania ciągłości działania.

Do skutecznej identyfikacji i pomiaru ryzyka wykorzystuje się następujące narzędzia:

1. Rejestr zdarzeń i strat operacyjnych
2. Rejestr skarg i reklamacji klientów Banku
3. Wyniki testów (ciągłości działania ,planów awaryjnych)
4. Wyników kontroli wewnętrznej
5. Wyników audytu zewnętrznego
6. Kluczowe wskaźniki ryzyka KRI

1. W ramach zarządzania ryzykiem operacyjnym Bank przeprowadza testy warunków skrajnych.
2. Przy konstrukcji założeń testów warunków skrajnych Bank bierze pod uwagę takie czynniki jak:
    a. Możliwe do nałożenia na Bank kary finansowe, wynikające z niedostatecznego dostosowania regulacji wewnętrznych do zmian przepisów zewnętrznych,
    b. Możliwości wystąpienia nadużyć wewnętrznych i zewnętrznych,
    c. Konsekwencje finansowe nieprawidłowości w obsłudze klienta – koszty rozpatrywania skarg i reklamacji,
    d. Awarie systemów oraz uszkodzenia aktywów które mogą mieć wpływ na wzrost kosztów działania Banku.
3. Testy warunków skrajnych są przeprowadzane w Banku na podstawie założeń zapewniających rzetelną ocenę ryzyka.
4. W celu przeprowadzenia testu warunków skrajnych Bank zakłada trzykrotny wzrost wartości strat w badanym okresie; jeżeli tak wyliczona kwota strat operacyjnych przekracza utworzony wewnętrzny wymóg kapitałowy to należy opracować plan działań zaradczych i ocenić zabezpieczenia możliwych strat rezerwą lub dodatkowym kapitałem wewnętrznym.
5. Test warunków skrajnych przeprowadzany jest w cyklach rocznych i stanowi element raportu ryzyka operacyjnego według wzoru:

∑ strat z tytułu ryzyka operacyjnego x 2 < wskaźnik bazowy ryzyka operacyjnego

Za istotny wpływ uznaje się wykorzystanie wskaźnika bazowego ryzyka operacyjnego na poziomie ≥ 90%.

6. Za przeprowadzenie testu warunków skrajnych odpowiedzialna jest Komórka monitorująca ryzyko.
7. Przeprowadzone testy warunków skrajnych oraz testy ciągłości działania są podstawą do weryfikacji funkcjonujących w Banku planów ciągłości działania oraz planów awaryjnych.

W zakresie bezpieczeństwa środowiska teleinformatycznego ryzyko operacyjne rozumiane jest jako wartość zależna od wpływu potencjalnych strat wynikających z niewłaściwego przetwarzania informacji i od prawdopodobieństwa wystąpienia takich strat.
Do szacowania ryzyka przyjęte zostały zalecenia zgodnie z ISO/IEC 27000:2009, w której opisane są wytyczne dotyczące zarządzania ryzykiem w bezpieczeństwie informacji.
W celu szacowania ryzyka Bank dokonuje systematycznej oceny zagrożeń i podatności przed i po zmaterializowaniu się zagrożenia.
Identyfikacja ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego jest przeprowadzana każdorazowo w przypadku planowania istotnych zmian w systemach informatycznych i ich wykorzystaniu oraz w przypadku wdrożenia nowych technologii.
Bank rozróżnia następujące komponenty systemu teleinformatycznego:

a. Sprzęt,
b. Oprogramowanie,
c. Sieć.

8. Szacowanie ryzyka odbywa się z uwzględnieniem klasyfikacji informacji i systemów informatycznych. Zasady klasyfikacji zdefiniowano w Instrukcji bezpieczeństwa środowiska teleinformatycznego i informacji w Banku Spółdzielczym w Łukowie.
   W rejestrze zdarzeń wewnętrznych w minionym roku nie zanotowano istotnych zdarzeń ryzyka operacyjnego.

   Planowane dalsze działania mające na celu ograniczenie występowania czynników ryzyka:

1. oferowanie klientom rachunków oraz zleceń stałych w celu zmniejszania ilości wpłat kasowych oraz przelewów bezgotówkowych,
2. przeprowadzenie szkoleń z zakresu technik aktywnej sprzedaży w Banku.
3. Testowanie systemów komputerowych na kopii zapasowej.

Lista potencjalnych zdarzeń ryzyka operacyjnego podlegających rejestracji w banku:

1. Oszustwa wewnętrzne
   a. Działania nieuprawnione
   b. Kradzież i oszustwo

2. Oszustwa zewnętrzne
    a. Kradzież i oszustwo
    b. Bezpieczeństwo systemów
3. Zasady dotyczące zatrudnienia oraz bezpieczeństwo w miejscu pracy
    a. Stosunki pracownicze
    b. Bezpieczeństwo środowiska pracy
    c. Podziały i dyskryminacja
4. Klienci, produkty i praktyki operacyjne
    a. Obsługa klientów, ujawnianie informacji o klientach, zobowiązania względem klientów
    b. Niewłaściwe praktyki biznesowe lub rynkowe
    c. Wady produktów
    d. Klasyfikacja klientów i ekspozycje
    e. Usługi doradcze
5. Szkody związane z aktywami rzeczowymi
    a. Klęski żywiołowe i inne zdarzenia
6. Zakłócenia działalności banku i awarie systemów
    a. Systemy
7. Wykonanie transakcji, dostawa i zarządzanie procesami operacyjnymi
    a. Wprowadzanie do systemu, wykonywanie, rozliczanie i obsługa transakcji
    b. Monitorowanie i sprawozdawczość
    c. Napływ i dokumentacja klientów
    d. Zarządzanie rachunkami klientów
    e. Kontrahenci niebędący klientami banku (np. izby rozliczeniowe)
    f. Sprzedawcy i dostawcy

Szczegółowe informacje ryzyka operacyjnego zawarte są w Zasadach zarządzania ryzykiem operacyjnym ,które jest udostępnione wszystkim zainteresowanym w formie papierowej w Centrali Banku Spółdzielczego w Łukowie ul. Chopina w Sekretariacie.