Załącznik do Uchwały nr 11/23 Zarządu Banku Spółdzielczego w Czarnym Dunajcu z dnia 19.01.2023r.

Zaktualizowano Uchwałą Zarządu nr 13/24 z dnia 26.01.2024r.

Załącznik do Uchwały nr 12/2023 Rady Nadzorczej Banku Spółdzielczego w Czarnym Dunajcu z dnia 30.01.2023r.

Zaktualizowano Uchwałą Rady Nadzorczej nr 9/2024 z dnia 29.01.2024r.

Polityka zgodności w Banku Spółdzielczym w Czarnym Dunajcu

Czarny Dunajec 2024

Spis treści

Rozdział 1. Postanowienia ogólne

§ 1.

Cel i zakres Polityki

1. Celem niniejszej „Polityki zgodności w Banku Spółdzielczym w Czarnym Dunajcu”, zwana dalej „Polityką” jest zapewnienie zgodności działania Banku z przepisami prawa, regulacjami wewnętrznymi Banku i standardami rynkowymi odpowiednio poprzez: adekwatną i skuteczną funkcję kontroli oraz zarządzanie ryzykiem braku zgodności, skutkujące utrzymaniem ryzyka braku zgodności na akceptowalnym przez Zarząd oraz Radę Nadzorczą poziomie.
2. Niniejsza polityka określa:
   1) podstawowe zasady zapewniania zgodności działania Banku z przepisami prawa, regulacjami wewnętrznymi Banku i standardami rynkowymi przez wszystkich pracowników Banku, w tym role i odpowiedzialność komórek organizacyjnych na pierwszej i drugiej linii obrony;
   2) obszary, które Bank uznaje za istotne z punktu widzenia zapewnienia zgodności;
   3) główne elementy procesu zarządzania ryzykiem braku zgodności, tzn. identyfikowania ryzyka braku zgodności; oceny przez pomiar lub ocenę tego ryzyka; projektowanie i wprowadzanie, bazujących na ocenie ryzyka braku zgodności mechanizmów kontroli ryzyka braku zgodności; monitorowanie wielkości i profilu ryzyka braku zgodności, po zastosowaniu mechanizmów kontroli ryzyka braku zgodności; okresowego przekazywania raportów w zakresie ryzyka braku zgodności do Zarządu i Rady Nadzorczej lub Komitetu audytu;
   4) rodzaje działań podejmowanych w przypadku wykrycia nieprawidłowości w stosowaniu Polityki, w tym środki naprawcze i dyscyplinujące;
   5) zakres, częstotliwość i adresatów informacji dotyczących zadań odnośnie zapewniania zgodności, w tym raportów w sprawie zarządzania ryzykiem braku zgodności.

§ 2.

Podstawy prawne i regulacyjne

Podstawą do sporządzenia niniejszej Polityki stanowią następujące przepisy prawne lub nadzorcze:

1) Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe;
2) Rozporządzenie Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 8 czerwca 2021 r. w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej oraz polityki wynagrodzeń w bankach;
3) Rekomendacja H dotyczącej systemu kontroli wewnętrznej w bankach, wydanej przez Komisję Nadzoru Finansowego w 2017 r.;
4) Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach, wydana przez Komisję Nadzoru Finansowego w 2013 r.;
5) Rekomendacja Z dotycząca zasad ładu wewnętrznego w bankach wydana przez Komisję Nadzoru Finansowego w 2020 r.;
6) Zasady Ładu Korporacyjnego dla Instytucji Nadzorowanych wydane przez Komisję Nadzoru Finansowego w 2014 r.
7) Kodeks Etyki Bankowej Związku Banków Polskich

§ 3.

Definicje

Użyte w Polityce definicje i określenia oznaczają:

1) **Audyt wewnętrzny** – wyodrębniona w ramach systemu kontroli wewnętrznej Banku, niezależna i obiektywna działalność doradcza i zapewniająca komórki audytu wewnętrznego, mająca na celu przysporzenie wartości i usprawnienie procesów w Banku oraz dokonywanie oceny adekwatności i skuteczności systemu zarządzania ryzykiem i systemu kontroli wewnętrznej (Rekomendacja H KNF) – w Banku jest to realizowana na trzeciej linii obrony działalność komórki audytu wewnętrznego SSOZ BPS;
2) **Bank** – Bank Spółdzielczy w Czarnym Dunajcu;
3) **Centrala Banku** – należy przez to rozumieć jednostkę organizacyjną Banku, usytuowaną w siedzibie Banku, wykonującą funkcję nadzorczą w stosunku do pozostałych jednostek organizacyjnych Banku oraz realizującą kluczowe dla całości Banku zadania merytoryczne i organizacyjne;
4) **Dokumentacja zewnętrzna –** dokumenty opracowane przez Bank i przekazywane klientom, kontrahentom i osobom trzecim, np. wzory umów, schemat wyciągów bankowych, broszury reklamowe, informacje prasowe, informacje w witrynach internetowych (Rekomendacja M KNF);
5) **Jednostka organizacyjna** - zasadniczy element struktury organizacyjnej, wydzielony ze względu na funkcje w organizacji lub według innych kryteriów (np. geograficznych lub produktowych) (Rekomendacja H KNF) - jednostkami organizacyjnymi są np.: Centrala, Oddziały, jednostki organizacyjne mogą być również wydzielane w strukturze organizacyjnej jednostek organizacyjnych wyższego rzędu - np. filie w ramach oddziałów, punkty kasowe, w ramach oddziałów lub filii, itp.
6) **Komórka organizacyjna** – jedno- lub wieloosobowy element struktury organizacyjnej wydzielony w ramach jednostki organizacyjnej dla realizacji określonych zadań, w tym także projektów (Rekomendacja H KNF);
7) **Komórka zgodności** - komórka ds. zgodności funkcjonująca w Banku;
8) **Linie obrony**– zorganizowanie w Banku systemu zarządzanie ryzykiem zarządzania ryzykiem i system kontroli wewnętrznej na trzech, niezależnych poziomach, o których mowa w §3 Rozporządzenia Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 8 czerwca 2021 r. w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej oraz polityki wynagrodzeń w bankach, na które składa się: **pierwsza linia obrony (inaczej pierwszy poziom)** obejmująca zarządzanie ryzykiem w działalności operacyjnej Banku, a także **druga linia obrony** (inaczej drugi poziom) - działalność komórki zgodności, a także innych komórek drugiej linii obrony, np. odpowiedzialnych za zarządzanie ryzykiem, bezpieczeństwo, itp;
9) **Mechanizm kontrolny** – wyróżnione w ramach funkcji kontroli, rozwiązanie lub działanie wykonywane i stosowane w ramach wszystkich linii obrony, w tym zwłaszcza w ramach pierwszej linii obrony, mające za zadanie zapewnienie osiągania celów systemu kontroli wewnętrznej (Rekomendacja H KNF), w tym zapewnienie przestrzegania mechanizmów kontroli ryzyka braku zgodności;
10) **Mechanizm kontroli ryzyka** – wyróżnione w ramach systemu zarządzania ryzykiem, rozwiązanie lub działanie wykonywane i stosowane w ramach pierwszej i drugiej linii obrony, mające na celu utrzymanie ryzyka na określonym poziomie (Rekomendacja H KNF);
11) **Mechanizm kontroli ryzyka braku zgodności** - mechanizmy kontroli ryzyka braku

zgodności wymienione w § 38 pk. 6 Rozporządzenia Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 8 czerwca 2021 r. w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej oraz polityki wynagrodzeń w bankach mechanizmy bazujące na ocenie ryzyka braku zgodności, mające na celu utrzymanie ryzyka braku zgodności na akceptowalnym poziomie (np. analiza nowych ryzyka produktów, uzyskiwanie opinii prawnej, wydawanie i monitorowanie zaleceń po testach komórki zgodności, szkolenia pracowników, inne mechanizmy i działania planowane i wdrażane w Banku ograniczające ryzyko braku zgodności);

12) **Naruszenie** – działanie lub zaniechanie pracowników Banku, powodujące niezgodność z przepisami prawa, regulacjami wewnętrznymi Banku (w tym zasadami etyki, zasadami w zakresie unikania konfliktu interesów) i standardami rynkowymi (np. Zasadami Ładu Korporacyjnego, Kodeksem Etyki Bankowej Związku Banków Polskich);
13) **Proces zarządzania ryzykiem braku zgodności** – realizowany przez komórkę zgodności (przy ewentualnym wsparciu innych komórek pierwszej lub drugiej linii obrony), proces identyfikacji, oceny, kontroli i monitorowania ryzyka braku zgodności działalności Banku z przepisami prawa, regulacjami wewnętrznymi i standardami rynkowymi oraz przedstawianie raportów w tym zakresie (Rekomendacja H KNF);
14) **Rada Nadzorcza** – Rada Nadzorcza Banku;
15) **Ryzyko braku zgodności** – ryzyko skutków nieprzestrzegania przepisów prawa, regulacji wewnętrznych oraz standardów rynkowych w procesach funkcjonujących w Banku (Rekomendacja H KNF);
16) **Ryzyko inherentne** – samoistne ryzyko wystąpienia danego zdarzenia lub okoliczności. Ryzyko to jest rodzajem ryzyka naturalnie związanego z działalnością prowadzoną przez Bank;
17) **Ryzyko resztkowe** – ryzyko pozostające po zastosowaniu mechanizmów kontroli ryzyka;
1) **Skutki finansowe –** poniesione, możliwe do ustalenia w dokładnie określonej wysokości (w złotych) straty spowodowane zdarzeniami ryzyka braku zgodności, do strat finansowych można zaliczyć zapłacone kary, odsetki karne, odszkodowania z tytułu materializacji ryzyka braku zgodności;
2) **Skutki niefinansowe –** trudno mierzalne skutki występowania ryzyka braku zgodności, objawiające się niezadowoleniem klientów, utratą dobrego wizerunku banku i naruszeniem reputacji, itp.,
3) **System ochrony** - należy przez to rozumieć system ochrony, o którym mowa ustawie z dnia 7 grudnia 2000 r. o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających (Rekomendacja H KNF);
4) **Testowanie** – porównywanie na wybranej próbie testowej stanu faktycznego ze stanem wymaganym, dokonywane w celu oceny co najmniej przestrzegania mechanizmów kontrolnych w odniesieniu do zakończonych czynności wykonywanych w ramach procesów funkcjonujących w Banku lub poszczególnych etapów tych czynności. Testowanie, jako element niezależnego monitorowania w ramach funkcji kontroli, może być monitorowaniem poziomym (testowanie poziome w ramach danej linii obrony) lub monitorowaniem pionowym (testowanie pionowe pierwszej linii obrony przez drugą linię obrony);
5) **Uniwersum compliance** - zbiór kluczowych obszarów działalności Banku oraz przepisów prawnych i standardów rynkowych będący przedmiotem działania komórki zgodności, w zakresie zapewniania celu głównego systemu kontroli wewnętrznej „przestrzeganie przepisów prawa, regulacji wewnętrznych oraz standardów rynkowych”;

6) **Weryfikacja bieżąca** – porównywanie stanu faktycznego ze stanem wymaganym, dokonywane w celu oceny co najmniej przestrzegania mechanizmów kontrolnych, przed rozpoczęciem lub w trakcie trwających czynności wykonywanych w ramach procesów funkcjonujących w banku. Weryfikacja bieżąca, jako element niezależnego monitorowania w ramach funkcji kontroli, może być monitorowaniem poziomym (weryfikacja bieżąca pozioma w ramach danej linii obrony) lub monitorowaniem pionowym (weryfikacja bieżąca pionowa pierwszej linii obrony przez drugą linię obrony).Weryfikacja bieżąca może być też realizowana jako nadzór służbowy, a także wiążące opiniowanie (udokumentowaną ocenę i zatwierdzanie) rozwiązań proponowanych przez innego pracownika lub komórkę organizacyjną.
7) **Zapewnianie zgodności** – zapewnianie przestrzegania przepisów prawa, regulacji wewnętrznych oraz standardów rynkowych, odpowiednio poprzez funkcję kontroli oraz zarządzanie ryzykiem braku zgodności (Rekomendacja H KNF);
8) **Zgodność -** (nazywana czasem z ang. compliance) w rozumieniu niniejszej Polityki oznacza zgodność działania Banku jako instytucji, a także zgodność działań podejmowanych przez osoby zatrudnione w Banku lub członków organów Banku z obowiązującymi przepisami prawa, regulacjami wewnętrznymi Banku, standardami rynkowymi;
9) **Zarząd** – Zarząd Banku.

Rozdział 2. Ryzyko braku zgodności, apetyt na ryzyko

§ 4.

Ryzyko braku zgodności, apetyt na ryzyko

Ryzyko braku zgodności - obejmuje skutki nieprzestrzegania przepisów prawa, regulacji wewnętrznych oraz standardów rynkowych w procesach funkcjonujących w Banku (Rekomendacja H KNF), skutki ryzyka mogą przybierać postać skutków finansowych oraz niefinansowych.

§ 5

Wszelkie działania Banku lub pracowników naruszające przepisy prawa lub standardy rynkowe, brak przestrzegania regulacji wewnętrznych prowadzący do naruszenia prawa lub standardów rynkowych, mogą prowadzić do naruszenia wizerunku Banku jako instytucji wiarygodnej i uwzględniającej w swych działaniach zasady legalności i etycznego postępowania i mogą spowodować negatywne skutki w postaci:

1) finansowe w postaci kar, zasądzonych odszkodowań skutkujące bezpośrednią stratą finansową,
2) niefinansowe – w postaci utraty reputacji lub osłabienia wizerunku Banku o sile oddziaływania dużo bardziej dotkliwej niż bezpośrednie straty finansowe.

§ 6

Nawet pozornie drobne naruszenia zgodności mogą doprowadzić, np. na skutek działań osób dotkniętych naruszeniem, informacji medialnych, itp. do powstania skandalu lub tzw. „czarnego scenariusza" - skutkującego postępowaniem organów kontrolnych, nadzorczych zakończonych karami lub innymi rodzajami dotkliwych sankcji dla Banku lub negatywnym odbiorem społecznym - w konsekwencji powodując znaczy wzrost ryzyka reputacji lub

negatywny wpływ na wyniki finansowe Banku, powstanie zagrożeń dla realizacji strategii rozwoju, a nawet katastrofalne skutki dla bezpiecznego funkcjonowania Banku.

§ 7

1. Ryzyko braku zgodności jest ryzykiem trudnomierzalnym, wobec tego zgodnie z § 14. ust. 2 Rozporządzenia Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 8 czerwca 2021 r. w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej oraz polityki wynagrodzeń w bankach - akceptowalna wartość ryzyka jest wyrażana w postaci miar jakościowych.
2. Bank akceptuje (obejmuje limitem) występowanie ryzyka braku zgodności na poziomie ryzyka resztkowego - NISKIE w zakresie wszystkich istotnych procesów Banku.
3. Ryzyko NISKIE oznacza poziom ryzyka, który powoduje:
   1) incydenty niezgodności:
      a) występujące rzadziej niż raz na 5 lat (częstotliwość – NISKIE – 1 pkt),
      b) przy skutkach ryzyka w rodzaju (ŚREDNIE – 2 pkt):
         - skutki nie finansowe - konsekwencje prawne w postaci powództwa indywidualnego, konsekwencje regulatora w postaci wydanego zalecenia, wystąpienia groźby utraty reputacji w postaci informacji w mediach lokalnych,

           lub

         - skutki finansowe - straty finansowe o wielkości mniejszej od 15% wyniku planowanego brutto;

   albo

   2) incydenty niezgodności:
      a) występujące od raz do roku do raz na 5 lat (ŚREDNIE – 2 pkt)
      b) przy skutkach ryzyka w rodzaju (NISKIE – 1pkt):
         - skutki niefinansowe - konsekwencje prawne w postaci skarg na naruszenie prawa lub regulacji i sporów, które (w każdym w wymienionych przypadków) można rozwiązać drogą mediacji, brak konsekwencji ze strony regulatora w postaci wydania zaleceń nadzorczych, brak groźby utraty strat reputacji z powodu postaci negatywnych informacji w mediach;

         lub

         - skutki finansowe wystąpienie materialnych strat finansowych mniejszych równych 5% wyniku planowanego brutto.

§ 8

Kluczowe obszary zarządzania ryzykiem braku zgodności (uniwersum compliance)

W Banku identyfikuje się następujące istotne obszary zarządzania ryzykiem braku zgodności wpływające na tzw. uniwersum compliance:

1) ochrona konsumenta i przeciwdziałanie nieuczciwej konkurencji, w tym:
   a) stosowanie wzorców umów pozbawionych niedozwolonych klauzul umownych (tzw. klauzul abuzywnych);
   b) wprowadzanie nowych produktów i modeli biznesowych, bez ryzyka obchodzenia powszechnie obowiązujących przepisów (Rek. M 14.6);
   c) uczciwa reklama produktów i działalności Banku;

2) przeciwdziałanie praniu pieniędzy i finansowaniu terroryzmu oraz przestrzeganie sankcji międzynarodowych, w tym w zakresie wynikającym z Rek. M KNF pkt. 14.6;
3) zapobieganie konfliktom interesów, w tym konfliktowi personalnemu i działalności konkurencyjnej pracowników Banku;
4) prawidłowe rozpatrywanie skarg i reklamacji;
5) realizacja obowiązków informacyjnych względem klientów zgodnie z przepisami, wynikająca z:
   a) Ustawy o kredycie konsumenckim,
   b) Ustawy o kredycie hipotecznym,
   c) Ustawy o usługach płatniczych,
   d) Polityki bancassurance – Rek. U KNF,
   e) obowiązku rzetelnego informowania o ryzyku produktów – w tym Rek. S KNF
6) prawidłowa realizacja Polityki wynagrodzeń;
7) prawidłowa realizacja Polityki informacyjnej, w tym realizacji obowiązków prawnych oraz objętych przepisami Rekomendacji Z KNF.

Rozdział 3. Dobre praktyki i kultura organizacyjna w zakresie zapewniania zgodności

§ 9
Dobre praktyki w zakresie zapewniania zgodności

Zarząd podkreśla istnienie obowiązków pracowników w zakresie:
1) obowiązku przestrzegania regulacji wewnętrznych obowiązujących w Banku;
2) przestrzegania zasad etyki przyjętych w Banku;
3) szczególnych przepisów prawa dotyczących działania Banku, w tym zasad ochrony tajemnicy bankowej, ochrony danych osobowych, przepisów dotyczących zapobiegania praniu pieniędzy i finansowaniu terroryzmu, przepisów o rachunkowości, a także wszelkich innych przepisów wymagających od Banku lub jego pracowników zachowania staranności;
4) unikania narażania Banku na negatywne oddziaływanie opinii klientów w reakcji na działania Banku związane z zarządzaniem ryzykiem braku zgodności.

§ 10
Kultura organizacyjna

1. Zarząd Banku podejmuje działania zmierzające do stworzenia i utrzymania kultury organizacyjnej, w której nacisk kładzie się na efektywne zarządzanie ryzykiem braku zgodności, przestrzeganie zasad i procedur oraz stosowanie ustalonych reguł postępowania, w tym ochronę przed utratą dobrej reputacji Banku.
2. Ryzyko braku zgodności - w odróżnieniu od innych rodzajów ryzyka, takich jak ryzyko kredytowe, czy rynkowe – obejmuje działanie wielu komórek i obszarów działalności Banku, w tym zarówno komórek i jednostek pierwszej linii obrony, jak i drugiej linii obrony.
3. Bank poprzez budowę kultury organizacyjnej ukierunkowanej na właściwe postępowanie z ryzykiem zmierza do aktywnego włączania się każdego pracownika w zarzadzanie ryzykiem braku zgodności.
4. Podstawową rolę odgrywa działanie kadry kierowniczej Banku, z uwagi na najważniejsze elementy kształtowania kultury organizacyjnej w zakresie zarządzania ryzykiem braku zgodności wdrażane w Banku, w postaci:
   1) odpowiednich zachowań i postawy kierownictwa, tzw. „przykład z góry”,

2) promowanie znajomości i stosowania zasad etycznego działania ,
3) jasne przypisanie i komunikowanie pracownikom ustalonych zadań i celów,
4) szkolenia i dzielenie się wiedzą,
5) ustalenie zasad oceny działalności, w tym promujących rzetelną realizację zadań
6) organizacja sposobu podejmowania decyzji zapobiegająca nieprawidłowościom,
7) delegowanie uprawnień i odpowiedzialności na niższe szczeble
8) uświadomiona odpowiedzialność pracowników za ryzyko braku zgodności.

Rozdział 4. Organizacja w zakresie zapewniania zgodności

§ 11

Poziomy zarządzania (linie obrony)

1. System zarządzania ryzykiem braku zgodności jest organizowany w Banku na trzech, niezależnych poziomach (liniach obrony), których struktura oraz jednoznaczne przypisanie komórek do poszczególnych linii obrony, zostało ustalone w Regulaminie organizacyjnym.
2. Pierwsza linia obrony – obejmuje działanie komórek i jednostek organizacyjnych pierwszego poziomu, w tym:
   1) bieżące zapewnianie zgodności w toku operacji – poprzez odpowiednie stosowanie mechanizmów kontroli ryzyka braku zgodności (np. przeglądy zarządcze, udział w sporządzaniu analizy luk regulacyjnych, wydawanie zaleceń po dokonanych testach poziomych pierwszej linii obrony, dostarczanie danych do wyznaczania wartości wskaźników ryzyka braku zgodności) oraz mechanizmów kontrolnych (np. procedur, podziału zadań, autoryzacji operacji, uzyskiwania autoryzacji projektów regulacji wewnętrznych, produktów, itp) a także przestrzeganie przepisów prawa, nadzorczych i regulacji wewnętrznych;
   2) dbałość o zgodność w toku projektowania regulacji wewnętrznych dotyczących realizacji procesów Banku, w przypadku projektowania przez komórki organizacyjne pierwszej linii;
   3) udział w realizacji procesu zarządzania ryzykiem braku zgodności – np. w zakresie przekazywania informacji służących do pomiaru ryzyka, a także zgłaszania naruszeń zgodności;
   4) niezależne monitorowanie przestrzegania mechanizmów kontrolnych w ramach monitorowania poziomego (weryfikacja bieżąca oraz testy poziome),
3. Druga linia – obejmuje działanie komórki zgodności, a także współpracujących w nią innych komórek drugiej linii obrony (np. Inspektora Ochrony Danych, Stanowiska ds. zarządzania ryzykami, Koordynatora PPPiFT), w zakresie:
   1) stosowania mechanizmów kontroli ryzyka braku zgodności (mechanizmów sterowania ryzykiem);
   2) stosowania mechanizmów kontrolnych dotyczących komórki zgodności – np. przestrzeganie regulacji wewnętrznych dotyczących działania komórki, w tym, zachowania podziału zadań, niezależności komórki, szkoleń pracowników;
   3) stosowania mechanizmów kontrolnych w zakresie zapewniania zgodności dotyczących innych komórek drugiej linii obrony (np. Inspektora Ochrony Danych, Stanowiska ds. zarządzania ryzykami, Koordynatora PPPiFT) – np. przestrzeganie regulacji wewnętrznych dotyczących działania komórek, w zakresie procedur działania, właściwego podziału zadań, uzyskiwania autoryzacji projektów regulacji wewnętrznych, szkoleń pracowników;

4) niezależne monitorowanie przestrzegania mechanizmów kontrolnych w ramach zadań komórki zgodności - weryfikacja bieżąca pozioma oraz testy poziome,
5) niezależne monitorowanie przestrzegania mechanizmów kontrolnych w ramach monitorowania pionowego innych komórek (np. Inspektora Ochrony Danych, Stanowiska ds. zarządzania ryzykami, Koordynatora PPPiFT - weryfikacja bieżąca pionowa oraz testy pionowe);
6) realizacji procesu zarządzania ryzykiem braku zgodności - identyfikacji, pomiaru, monitorowanie oraz raportowania na temat ryzyka.

4. Trzecia linia – niezależna ocena adekwatności i skuteczności procesu zarządzania ryzykiem braku zgodności poprzez działanie audytu wewnętrznego SSOZ BPS.

Rozdział 5. Zadania w zakresie zarządzania ryzykiem braku zgodności

§ 12

Zadania Rady Nadzorczej Banku

1. Rada Nadzorcza Banku sprawuje nadzór nad wprowadzeniem i zapewnianiem funkcjonowania adekwatnego i skutecznego systemu kontroli wewnętrznej, tym samym nadzoruje obszar zapewniania zgodności, w tym zarządzanie ryzykiem braku zgodności, będące elementem systemu kontroli wewnętrznej.
2. Rada Nadzorcza Banku zatwierdza akceptowalny poziom ryzyka braku zgodności.
3. W ramach zapewniania przez system kontroli wewnętrznej przestrzegania przepisów prawa, regulacji wewnętrznych oraz standardów rynkowych Rada Nadzorcza Banku:
   1) nadzoruje wykonywanie obowiązków przez Zarząd Banku dotyczących zarządzania ryzykiem braku zgodności,
   2) zatwierdza Politykę zarządzania zgodnością i ryzykiem braku zgodności w Banku Spółdzielczym, ponadto „Regulamin kontroli wewnętrznej Banku Spółdzielczego", a także „Regulamin funkcjonowania komórki zgodności".
   3) dokonuje corocznej oceny adekwatności i skuteczności systemu kontroli wewnętrznej, w tym adekwatności i skuteczności funkcji kontroli, komórki zgodności,
   4) co najmniej raz w roku ocenia stopień efektywności zarządzania ryzykiem braku zgodności przez Bank i informuje SSOZ BPS o wynikach tej oceny.
4. **Komitet audytu** – monitoruje skuteczność systemu kontroli wewnętrznej, opiniuje jego adekwatność i skuteczność.
5. W ramach nadzoru nad zarządzaniem ryzykiem braki zgodności Rada Nadzorcza Banku:
   1) ocenia adekwatność i skuteczność systemu kontroli wewnętrznej w oparciu o informacje uzyskane od komórki zgodności, audytu SSOZ BPS, Zarządu Banku, oraz Komitetu audytu
   2) nadzoruje i ocenia czynności wykonywane przez członków Zarządu Banku w związku z realizacją ich zadań w zakresie systemu zarządzania,
   3) nadzoruje przestrzeganie w Banku regulacji wewnętrznych w zakresie zapewniania zgodności.
6. Rada Nadzorcza Banku upewnia się, że wprowadzone przez Zarząd Banku rozwiązania organizacyjne oraz regulacje wewnętrzne mające na celu ograniczenie występowania konfliktu interesów i powiązań personalnych są odpowiednie i zapewniają w szczególności (Rekomendacja M KNF):
   1) rozdzielenie funkcji kierowania i zwierzchności organizacyjnej nad jednostkami operacyjnymi w banku (w tym uwzględniające podejmowanie decyzji w okresie zastępstw członków Zarządu Banku),
   2) niezależność i obiektywizm sprawowanej kontroli wewnętrznej,

3) przestrzeganie określonych w Banku zasad podejmowania decyzji przez osoby powiązane personalnie.

7. Wewnętrzny podział kompetencji wskazujący członka Zarządu Banku, do którego są zgłaszane naruszenia oraz odpowiedzialnego za bieżące funkcjonowanie *Procedury anonimowego zgłaszania naruszeń prawa oraz obowiązujących procedur i standardów etycznych w Banku Spółdzielczym* podlega zatwierdzeniu przez Radę Nadzorczą Banku.
8. Rada Nadzorcza Banku, w zależności od potrzeb, nie rzadziej jednak niż raz w roku, ocenia adekwatność i skuteczność *Procedury anonimowego zgłaszania naruszeń prawa oraz obowiązujących procedur i standardów etycznych w Banku Spółdzielczym*.

§ 13

Zadania Zarządu Banku

1. Zarząd Banku projektuje, wprowadza oraz zapewnia działanie systemu kontroli wewnętrznej - w tym w zakresie zapewniania zgodności oraz procedur anonimowego zgłaszania naruszeń prawa oraz obowiązujących w Banku regulacji wewnętrznych i standardów etycznych.
2. Zarząd Banku odpowiada za efektywne zarządzanie ryzykiem braku zgodności, w tym: opracowanie Polityki zgodności, zapewnienie jej przestrzegania i składanie sprawozdań Radzie Nadzorczej Banku w sprawie zarządzania w Banku ryzykiem braku zgodności.
3. Do obowiązków Zarządu Banku należy opracowanie, wdrożenie oraz zapewnianie funkcjonowania adekwatnego i skutecznego systemu kontroli wewnętrznej, w szczególności wyodrębnienie komórki zgodności oraz zapewnienie jej odpowiedniej niezależności i zasobów.
4. Zarząd Banku podejmuje działania, mające na celu zapewnienie ciągłości działania systemu kontroli wewnętrznej, w tym właściwej współpracy wszystkich pracowników Banku z komórką zgodności, oraz dostępu pracowników komórki do niezbędnych dokumentów źródłowych, w tym zawierających informacje poufne, w związku z wykonywaniem przez nich obowiązków służbowych.
5. W przypadku stwierdzenia nieprawidłowości w stosowaniu Polityki zgodności, Zarząd Banku podejmuje odpowiednie działania w celu usunięcia nieprawidłowości, w tym określone środki naprawcze lub dyscyplinujące.
6. Zarząd Banku jest odpowiedzialny za adekwatność i skuteczność *Procedury anonimowego zgłaszania naruszeń prawa oraz obowiązujących procedur i standardów etycznych*.
7. Zarząd Banku ustala wewnętrzny podział kompetencji wskazujący członka Zarządu Banku, do którego są zgłaszane naruszenia oraz odpowiedzialnego za bieżące funkcjonowanie procedury anonimowego zgłaszania naruszeń.
8. Zarząd Banku informuje nie rzadziej niż raz do roku Radę Nadzorczą Banku o sposobie wypełniania zadań w zakresie:
    1) adekwatności i skuteczności systemu kontroli wewnętrznej w zapewnianiu osiągania celów systemu kontroli wewnętrznej, w tym zapewniania zgodności,
    2) skali i charakteru nieprawidłowości znaczących i krytycznych oraz najważniejszych działań zmierzających do usunięcia tych nieprawidłowości, w tym podjętych środków naprawczych i dyscyplinujących,
    3) zapewniania niezależności komórce zgodności,
    4) zapewniania odpowiednich zasobów kadrowych niezbędnych do skutecznego wykonywania zadań oraz koniecznych środków finansowych do systematycznego podnoszenia kwalifikacji, zdobywania doświadczenia i umiejętności przez pracowników komórki zgodności.

§ 14
Zadania Komórki zgodności

1. W Banku funkcjonuje Komórka zgodności, będąca częścią drugiej linii obrony, ma ona charakter niezależny, funkcjonuje z odpowiednim uwzględnieniem zasady unikania konfliktu interesów, w tym niezależnie od działań pierwszej linii obrony.
2. Cel, zakres i szczegółowe zasady działania oraz strukturę organizacyjną Komórki zgodności w Banku określa „*Regulamin funkcjonowania komórki zgodności*" opracowany zatwierdzany przez Zarząd Banku oraz akceptowany Radę Nadzorczą Banku.
3. Komórka zgodności wykonuje czynności na podstawie *Regulaminu funkcjonowania komórki zgodności*, *Instrukcji zarządzania ryzykiem braku zgodności* oraz innych regulacji wewnętrznych dotyczących obszarów związanych z zarządzaniem ryzykiem braku zgodności.
4. Podstawowe zadania Komórki zgodności:
   1) opracowanie projektów regulacji wewnętrznych określających: cel, zakres i szczegółowe zasady działania oraz strukturę organizacyjną komórki, a także pisemne procedury, metodyki oraz dokumentowanie działań,
   2) opracowanie projektów regulacji wewnętrznych w zakresie zarządzania ryzykiem braku zgodności w Banku,
   3) dbałość o właściwe powiązanie zarządzania ryzykiem braku zgodności ze strategią Banku, w tym poprzez dokonywanie przeglądów zarządczych regulacji dotyczących działania komórki zgodności oraz w zakresie zarządzania ryzykiem braku zgodności,
   4) koordynowanie działań innych komórek i jednostek organizacyjnych w zakresie zarządzania ryzykiem braku zgodności,
   5) koordynowanie procesu informowania o zmianach w przepisach prawa, regulacjach wewnętrznych i standardach rynkowych,
   6) identyfikowanie ryzyka braku zgodności, w szczególności poprzez:
      - analizę przepisów prawa, regulacji wewnętrznych banku, standardów rynkowych,
      - analiza nowych produktów i usług wprowadzanych do oferty banku, analiza modyfikacji tych produktów i usług oraz analiza procesów sprzedażowych tych produktów i usług, pod kątem zgodności z przepisami prawa, regulacjami wewnętrznymi i standardami rynkowymi (np. analiza pod kątem zgodności z ustawą o kredycie konsumenckim, wymogami bancassurance, wymogami, przeciwdziałania tzw. missellingowi, itp),
      - przeprowadzanie w stosownych przypadkach wewnętrznych postępowań wyjaśniających;
   7) ocenę ryzyka braku zgodności poprzez pomiar lub szacowanie,
   8) kontrolę ryzyka braku zgodności, rozumianą jako oddziaływanie na jego poziom, poprzez działania podejmowane przez Komórkę, w zakresie:
      a) stosowania mechanizmów kontroli ryzyka braku zgodności, w tym opiniowanie procedur, skryptów, pism seryjnych w zakresie ich zgodności z regulacjami wewnętrznymi i powszechnie obowiązującymi przepisami prawa, a także określenie i monitorowanie wskaźników ryzyka braku zgodności,
      b) określania przez Komórkę rodzajów mechanizmów kontroli ryzyka braku zgodności stosowanych w Banku,
      c) wskazywanie komórek organizacyjnych (w tym zwłaszcza działające w ramach pierwszej linii obrony) odpowiedzialne za zaprojektowanie, wdrożenie i stosowanie poszczególnych rodzajów mechanizmów kontroli ryzyka braku zgodności w procesach, w których uczestniczą;

9) monitorowanie poziom ryzyka braku zgodności po zastosowaniu mechanizmów kontrolnych, o których mowa pkt. 6, w szczególności poprzez wykorzystanie wyników oceny ryzyka braku zgodności oraz przeprowadzanie testów zgodności,
10) okresowe raportowanie w zakresie ryzyka braku zgodności do Zarządu, Rady Nadzorczej, Komitetu audytu,
11) doradzanie Zarządowi i komórkom organizacyjnym w zakresie zgodności, bez naruszenia zasady unikania konfliktu interesów,
12) współpraca z komórkami wewnętrznymi Banku w zakresie oceny i monitorowania ryzyka braku zgodności, w tym z: *komórką ds. zarządzania ryzykami, Inspektorem Ochrony Danych, koordynatorem AML;,*
13) przyjmowanie zgłoszeń naruszenia prawa oraz obowiązujących procedur i standardów etycznych i zapewniania ochrony danych osób dokonujących zgłoszeń, jak również osób, którym zarzuca się dokonanie naruszenia,
14) monitorowanie i raportowanie statusu zaleceń wydanych dla Banku z wszystkich źródeł (audyt SSOZ, UKNF, UOKiK, zaleceń Wewnętrznych oraz Zewnętrznych) oraz raportowanie kwartalne o statusie realizacji do RN,
15) dokonywanie przeglądu wdrożenia polityki wynagrodzeń dokonywanemu nie rzadziej niż raz w roku. Raport z przeglądu przedstawiany jest Radzie Nadzorczej.

5. Osoba kierująca komórką do spraw zgodności lub osoby je zastępujące uczestniczą w posiedzeniach Zarządu. W przypadku, w którym osoba kierująca komórką ds. zgodności lub osoba zastępująca nie może uczestniczyć w posiedzeniu, powinna każdorazowo zapoznać się z protokołem posiedzenia Zarządu, jednakże w przypadku gdy przedmiotem posiedzenia są zagadnienia związane z systemem kontroli wewnętrznej, w tym zapewnienia zgodności, audytem wewnętrznym oraz zarządzaniem ryzykiem obecność jest obligatoryjna.
6. Komórce zgodności przysługuje w zakresie niezbędnym do realizacji obowiązków oraz w celu wzmocnienia niezależności funkcjonowania:
   1) prawo dostępu do wszelkich niezbędnych informacji i danych (w tym poufnych i wrażliwych) oraz do pomieszczeń w zakresie koniecznym do wykonywania zadań w obecności osób odpowiedzialnych za te pomieszczenia oraz prawo dostępu do systemów informatycznych (bez możliwości ingerencji w zasoby systemu) uwzględniających informacje i dane niezbędne do wykonywania zadań,
   2) prawo do żądania informacji i danych oraz otrzymywania niezwłocznych odpowiedzi od pracowników i komórek organizacyjnych posiadających te informacje i dane,
   3) prawo do wglądu do wszelkich akt i dokumentów oraz sporządzania kopii, odpisów lub wyciągów oraz do dokonywania oględzin, przeliczeń, pomiarów w zakresie koniecznym do wykonywania zadań,
   4) prawo do żądania pisemnych oraz ustnych wyjaśnień i oświadczeń oraz otrzymywania niezwłocznych odpowiedzi (bez zbędnych opóźnień) od pracowników banku, w związku z wykonywanymi zadaniami Komórki zgodności,
   5) prawo do uzyskiwania pomocy od pracowników odpowiednich komórek organizacyjnych banku w zakresie koniecznym do wykonywania zadań,
   6) możliwość stosowania narzędzi informatycznych wspomagających realizację zadań komórki do spraw zgodności,
   7) prawo do zamawiania ekspertyz zewnętrznych.
7. Ekspertyzy zewnętrzne są to wszelkie opinie prawne, doradztwo prawne, analizy, przeglądy problemowe. Wszelkie zlecenia ekspertyz zewnętrznych wraz z zakresem przedmiotowym są kierowane przez Komórkę ds. zgodności oraz poddawane akceptacji Prezesa Zarządu. Wyniki w/w czynności nie mogą być traktowane jako

zrealizowanie planu Compliance, bądź testowania pionowego przez komórkę ds. zgodności.

§ 15

Zadania komórek organizacyjnych drugiej linii

1. Właściwe merytorycznie komórki organizacyjne Banku należące do drugiej linii obrony (np. Inspektora Ochrony Danych, komórka ds. zarządzania ryzykami, Koordynatora PPPiFT), są odpowiedzialne m.in. za:
   1) przygotowanie projektów regulacji wewnętrznych, zgodnie z przepisami Instrukcji tworzenia aktów normatywnych w Banku Spółdzielczym w Czarnym Dunajcu, w tym w zgodności z przepisami prawa powszechnego, a także standardami rynkowymi w merytorycznych obszarach ich działania,
   2) identyfikację ryzyka braku zgodności poprzez analizę zapisów w opracowywanych przez daną komórkę regulacjach, ze szczególnym uwzględnieniem w umowach z klientami – konsumentami klauzul niedozwolonych (pojawienie się w rejestrze klauzul niedozwolonych nowej klauzuli wymaga przeprowadzenia – we współpracy z Radcą Prawnym – analizy jej występowania w umowach z klientami – konsumentami, ustalenia przedmiotowej analizy winny mieć formę pisemną) oraz zgłaszanie propozycji zmian w regulacjach wewnętrznych w aspekcie klauzul niedozwolonych,
2. Właściwe merytorycznie komórki organizacyjne Banku, zaliczone odpowiednio do drugiej linii obrony (np. Inspektora Ochrony Danych, komórka ds. zarządzania ryzykami, Koordynatora PPPiFT,, są też odpowiedzialne są m.in. za współpracę z Komórką zgodności w zakresie:
   1) identyfikacji i przekazywania informacji o występujących incydentach zgodności,
   2) ewidencji w systemie zdarzeń operacyjnych dotyczących ryzyka braku zgodności,
   3) dokonywania przeglądów zarządczych regulacji wewnętrznych Banku i przekazywanie ich wyników do Komórki zgodności w razie stwierdzenia niezgodności tych regulacji z przepisami lub innymi regulacjami Banku.
3. Właściwe merytorycznie komórki organizacyjne Banku, zaliczone do drugiej linii obrony odpowiedzialne są za stosowanie i monitorowanie mechanizmów kontrolnych drugiej linii obrony - w ramach funkcji kontroli realizowanej zgodnie z Regulaminem kontroli wewnętrznej, a także innymi regulacjami wewnętrznymi Banku, np. dotyczącymi realizacji nadzoru nad procesami, dokonywania przeglądów zarządczych, itp.

§ 16

Zadania jednostek i komórek organizacyjnych Banku - pierwszej linii

1. Właściwe merytorycznie komórki organizacyjne Banku, zaliczone do pierwszej linii obrony (np. komórki zaliczone do Pionu Handlowego) są odpowiedzialne m.in. za:
   1) przygotowanie projektów regulacji wewnętrznych, zgodnie z przepisami *Instrukcji* tworzenia aktów normatywnych w Banku Spółdzielczym w Czarnym Dunajcu, w tym w zgodności z przepisami prawa powszechnego, a także standardami rynkowymi w merytorycznych obszarach ich działania,
   2) identyfikację ryzyka braku zgodności poprzez analizę zapisów w opracowywanych przez daną komórkę regulacjach, ze szczególnym uwzględnieniem w umowach z klientami – konsumentami klauzul niedozwolonych (pojawienie się w rejestrze

klauzul niedozwolonych nowej klauzuli wymaga przeprowadzenia – we współpracy z Radcą Prawnym – analizy jej występowania w umowach z klientami – konsumentami, ustalenia przedmiotowej analizy winny mieć formę pisemną) oraz zgłaszanie propozycji zmian w regulacjach wewnętrznych w aspekcie klauzul niedozwolonych,

2. Właściwe merytorycznie komórki organizacyjne Centrali, zaliczone do pierwszej, są też odpowiedzialne są m.in. za współpracę z Komórką zgodności w zakresie:
   1) identyfikacji i przekazywania informacji o występujących incydentach zgodności,
   2) ewidencji w systemie zdarzeń operacyjnych dotyczących ryzyka braku zgodności,
   3) dokonywania przeglądów zarządczych regulacji wewnętrznych Banku i przekazywanie ich wyników do Komórki zgodności w razie stwierdzenia niezgodności tych regulacji z przepisami lub innymi regulacjami Banku.
3. Jednostki organizacyjne Banku pierwszej linii - wykonują zadania związane z bieżącym zapewnianiem zgodności, w tym zarządzaniem ryzykiem braku zgodności w toku swoich operacji, obejmuje to:
   1) odpowiednie stosowanie mechanizmów kontroli ryzyka braku zgodności,
   2) zgłoszenia naruszeń przepisów zgodnie z Procedurą anonimowego zgłaszania naruszeń prawa oraz obowiązujących procedur i standardów etycznych w Banku Spółdzielczym,
   3) realizację niezależnego monitorowania poziomego przestrzegania mechanizmów kontrolnych w zakresie zapewniania zgodności - zgodnie z Regulaminem kontroli wewnętrznej, a także innymi regulacjami wewnętrznymi Banku.

Rozdział 6. Proces zarządzania ryzykiem braku zgodności

§ 17

Wdrożenie Polityki

Działania służące realizacji Polityki realizowane w Banku polegają na:

1) organizacji procesu zarządzania ryzykiem braku zgodności zgodnie z regulacjami wewnętrznymi Banku zaakceptowanymi przez Zarząd i zgodnymi z przepisami niniejszej Polityki,
2) tworzeniu i zapewnianiu odpowiedniego środowiska zarządzania ryzykiem.

§ 18

Proces zarządzania ryzykiem braku zgodności

1. Proces zarządzania ryzykiem braku zgodności realizowany w Banku obejmuje:

   1) Identyfikację ryzyka – poprzez
      a) analizę przepisów prawa, regulacji wewnętrznych i standardów rynkowych - na podstawie uzyskiwania informacji wewnętrznych i zewnętrznych o wymaganiach w zakresie zgodności, np.
         - baz danych i informacji o zmianach aktów prawnych,
         - alertów prawnych z Banku Zrzeszającego oraz SSOZ BPS,
         - ewidencji regulacji wewnętrznych Banku,
      b) informacji dotyczących braku wdrożenia mechanizmów kontroli ryzyka braku zgodności lub mechanizmów kontrolnych,
      c) zgłoszonych anonimowo informacji dotyczących naruszania przepisów, regulacji wewnętrznych i przyjętych norm,
   2) ocenę ryzyka – poprzez jego pomiar lub szacowanie,

3) kontrolę ryzyka – poprzez projektowanie i wprowadzanie, bazujących na ocenie ryzyka braku zgodności, mechanizmów kontroli ryzyka braku zgodności,
4) monitorowanie – wielkości i profilu ryzyka braku zgodności, po zastosowaniu mechanizmów kontroli ryzyka braku zgodności,
5) raportowanie - na temat ryzyka braku zgodności – do Zarządu i Rady Nadzorczej oraz Komitetu audytu.

2. Regulacje wewnętrzne dotyczące procesu zarządzania ryzykiem braku zgodności powinny być znane pracownikom Banku uczestniczącym w procesie.
3. Regulacje wewnętrzne podlegają regularnej weryfikacji, w celu ich dostosowania do mian profilu ryzyka Banku, a także otoczenia gospodarczego, prawnego i regulacyjnego, w którym Bank działa.

§ 19

Środowisko zarządzania ryzykiem

Środowisko zarządzania ryzykiem braku zgodności zapewniane w Banku obejmuje:
1) tworzenie kultury organizacyjnej, zorientowanej na właściwe postępowanie z ryzykiem, w tym: ustalenie zasad w postaci niniejszej Polityki i innych regulacji wewnętrznych, wykonywanie zadań kierownictwa obejmujących promowanie dobrych postaw, nadzór nad podwładnymi i ryzykiem ich działań,
2) właściwą strukturę organizacyjną i podział zadań,
3) zapewnienie odpowiednich zasobów, w tym wyodrębnienie i zapewnienie zasobów dla działania Komórki zgodności, a także zapewnienie uprawnień i niezależności Komórki zgodności,
4) zapewnienie odpowiednich zasobów informatycznych, w tym dostępu do baz danych lub informacji dotyczących zmian prawnych,
5) zapewnienie sprawnego przepływu informacji i raportowania wewnętrznego.
6) szkolenia.

Rozdział 7. Monitorowanie ryzyka braku zgodności

§ 20

Monitorowanie ryzyka

Dokonywane jest monitorowanie ryzyka w celu:
1) ustalenia zmiany wielkości i profilu ryzyka na skutek zastosowania środków kontroli ryzyka braku zgodności (ryzyka rezydualnego, ryzyka resztkowego), w stosunku do ustalonego na podstawie pierwotnej identyfikacji i oceny poziomu ryzyka (ryzyka inherentnego);,
2) kontroli i oceny wcześniejszych etapów procesu zarządzania ryzykiem, tzn. identyfikowania, szacowania i stosowania mechanizmów kontrolnych dla ustalenia ich skuteczności - celem oceny adekwatności i skuteczności procesu.

§ 21

Profil i akceptowalny poziom ryzyka braku zgodności

1. Profil ryzyka braku zgodności rozumiany jest jako określenie skali narażenia Banku na negatywne zdarzenia z zakresu ryzyka braku zgodności, które mogą powodować lub powodują negatywne dla Banku konsekwencje tj. koszty finansowe i niefinansowe w ramach głównych obszarów ryzyka (procesów istotnych). Profil ryzyka braku zgodności, określa skalę i strukturę ekspozycji na ryzyko braku zgodności, a także ryzyko resztkowe pozostające po zastosowaniu mechanizmów kontroli ryzyka.
2. Zarząd Banku ustala akceptowalny poziom ryzyka braku zgodności, który jest zatwierdzany przez Radę Nadzorczą.
3. Akceptowalny poziom ryzyka braku zgodności należy rozumieć jako całkowite ryzyko, na które Bank jest gotowy i które jest skłonny podjąć a priori (co niekiedy nazywane jest apetytem na ryzyko braku zgodności). Akceptowalny poziom ryzyka przyjęty w Banku jest określony w § 7 ust. 3.
4. Przestrzeganie akceptowalnego poziomu ryzyka braku zgodności podlega kwartalnemu monitorowaniu oraz raportowaniu tego zagadnienia Radzie Nadzorczej, Zarządowi.
5. Komórka ds. zgodności dokonuje w cyklach rocznych w terminie do końca lutego danego roku weryfikacji profilu ryzyka braku zgodności oraz akceptowalnego poziomu ryzyka braku zgodności.

§ 22

Monitorowanie przestrzegania akceptowalnego poziomu ryzyka

1. Do oceny profilu ryzyka braku zgodności Bank wykorzystuje:
   1) informacje na temat naruszeń zgodności, w tym poziom strat finansowych i pozafinansowych;
   2) informacje o zmianach przepisów prawnych lub regulacji wewnętrznych,
   3) informacje dotyczące nieprawidłowości stosowania lub braku wdrożenia mechanizmów kontroli ryzyka braku zgodności lub mechanizmów kontrolnych,
   4) zgłoszonych anonimowo informacji dotyczących naruszania przepisów i przyjętych norm,
   5) analizy wskaźników ryzyka braku zgodności.

2. W przypadku, gdy zidentyfikowana wielkość ryzyka braku zgodności jest wysoka lub krytyczna, niezbędne informacje w tym zakresie powinny być przekazywane przez komórkę do spraw zgodności niezwłocznie do Zarządu i Rady Nadzorczej oraz co najmniej raz do roku, przekazywane do SSOZ BPS.

Rozdział 8. Rodzaje działań naprawczych i dyscyplinujących

§ 23

Zalecenia w przypadku wykrycia nieprawidłowości

1. Zarząd Banku określa rodzaje działań podejmowanych w celu usunięcia nieprawidłowości w stosowaniu Polityki wykrytych przez system kontroli wewnętrznej, w tym określone środki naprawcze i dyscyplinujące.
2. Do środków naprawczych należy wydawanie zaleceń pokontrolnych na odpowiednim szczeblu organizacyjnym, w szczególności obejmujących polecenie zaprojektowania nowych i aktualizacja dotychczasowych mechanizmów kontrolnych (np. zmiana procedury, modyfikacja poszczególnych procesów, szkolenia).
3. Zalecenia pokontrolne wydawane są zgodnie z zasadami Regulaminu kontroli wewnętrznej.

Rozdział 9. Raportowanie ryzyka braku zgodności

§ 24

Raportowanie ryzyka braku zgodności

1. Komórka zgodności przedkłada raporty kwartalne Zarządowi oraz Radzie Nadzorczej, a także Komitetowi audytu zgodnie z zasadami zawartymi w Regulaminie funkcjonowania Komórki zgodności w Banku Spółdzielczym.
2. Raporty Komórki obejmują:
   1) wyniki identyfikacji ryzyka braku zgodności, w tym obejmujących istotne zmiany w przepisach prawa, regulacjach wewnętrznych i standardach rynkowych
   2) wyniki oceny ryzyka braku zgodności, w tym obejmujących zestawienie ocen ryzyka braku zgodności wskazujących na wysoki poziom ryzyka braku zgodności,
   3) wyniki kontroli ryzyka braku zgodności (sterowania ryzykiem), w tym obejmujące zestawienie najważniejszych rodzajów mechanizmów kontroli ryzyka braku zgodności,
   4) wyniki monitorowania wielkości i profilu ryzyka braku zgodności, w tym obejmujące zestawienie statusów wdrożenia mechanizmów kontroli ryzyka braku zgodności, przypadków korekty oceny ryzyka braku zgodności oraz wyników testowania pionowego (w tym w zakresie wdrożenia i przestrzegania mechanizmów kontroli ryzyka).
3. W przypadku, gdy zidentyfikowana wielkość ryzyka braku zgodności jest wysoka lub krytyczna, niezbędne informacje w tym zakresie powinny być przekazywane przez komórkę zgodności niezwłocznie do Zarządu i Rady Nadzorczej oraz co najmniej raz do roku, przekazywane do SSOZ BPS.
4. Zarząd Banku jest niezwłocznie informowany o wykrytych nieprawidłowościach (błędach) typu P 1 (błąd krytyczny) oraz Typu P 2 (błąd znaczący) zgodnie z klasyfikacją ustaloną w Regulaminie kontroli wewnętrznej.

§ 25

Raportowanie Zarządu Banku do Rady Nadzorczej Banku i Komitetu Audytu

1. Rada Nadzorcza oraz Komitet Audytu otrzymuje nie rzadziej niż raz na kwartał sprawozdanie dotyczące poziomu ryzyka braku zgodności oraz proponowanych działań zapobiegawczych i redukujących ryzyko sporządzone przez komórkę ds. zgodności,
2. Rada Nadzorcza oraz Komitet Audytu otrzymują Roczne raporty z działalności komórki ds. zgodności,
3. Rada Nadzorcza otrzymuje nie rzadziej niż raz do roku sprawozdanie Zarządu dotyczące efektywności (adekwatności i skuteczności) zarządzania ryzykiem braku zgodności w Banku.
4. Rada Nadzorcza oraz Komitet Audytu jest niezwłocznie informowany o wykrytych przez komórkę ds. zgodności nieprawidłowościach (błędach) typu P 1 (błąd krytyczny) oraz typu P 2 (błąd znaczący) zgodnie z klasyfikacją ustaloną w Regulaminie kontroli wewnętrznej.

§ 26

Raportowanie wyników wewnętrznych postępowań wyjaśniających

Szczególnym rodzajem są raporty Komórki zgodności sporządzane doraźnie dotyczące wewnętrznych postępowań wyjaśniających, składane Zarządowi Banku oraz Radzie Nadzorczej Banku na skutek przeprowadzonego w Banku postępowania.

Rozdział 10. Kontrola zarządzania ryzykiem braku zgodności

§ 27

Kontrola wewnętrzna

Kontrola zapewniania zgodności, w tym funkcjonowania systemu zarządzania ryzykiem braku zgodności, dokonywana jest zgodnie z Regulaminem kontroli wewnętrznej.

§ 28

1. Kontrola działalności Komórki zgodności dokonywana jest przez audyt wewnętrzny SSOZ BPS.
2. Funkcja audytu wewnętrznego dla Uczestników Systemu Ochrony Zrzeszenia BPS jest realizowana przez Pion Audytu w Spółdzielni Systemu Ochrony Zrzeszenia BPS i jest uregulowana odrębnymi przepisami w tym zakresie.
3. Celem audytu wewnętrznego w Systemie Ochrony jest zapewnienie osiągnięcia celów Systemu Ochrony, m. in. poprzez badanie audytowe mające na celu weryfikację przestrzegania przez Spółdzielnię i Uczestników przepisów prawa, postanowień Umowy oraz zasad zarządzania ryzykiem.
4. Zasady prowadzenia audytu wewnętrznego w Systemie Ochrony określają „Zasady audytu wewnętrznego w Systemie Ochrony Zrzeszenia BPS", stanowiącej załącznik do Umowy Systemu Ochrony Zrzeszenia BPS.

Rozdział 10. Postanowienia końcowe

§ 29

1. Niniejsza Polityka podlega okresowym przeglądom i aktualizacji zgodnie z przepisami prawa nie rzadziej niż raz w roku przez Komórkę ds. zgodności.
2. Niniejsza Polityka wymaga zatwierdzenia przez Radę Nadzorczą.