

# **Zasady funkcjonowania systemu kontroli wewnętrznej w Prabutach**

## SPIS TREŚCI

DZIAŁ I.....	2
Rozdział 1 - Postanowienia ogólne .....	2
Rozdział 2 – Model trzech linii (poziomów) obrony .....	4
Rozdział 3 – Podział obowiązków .....	5
DZIAŁ II – Funkcja kontroli .....	8
Rozdział 1 – Cele systemu kontroli wewnętrznej .....	8
Rozdział 2 – Mechanizmy kontrolne .....	9
Rozdział 3 – Niezależne monitorowanie .....	11
DZIAŁ IV – Matryca funkcji kontroli .....	13
DZIAŁ V – Weryfikacja bieżąca kluczowych mechanizmów kontrolnych...	14
DZIAŁ VI – Testowanie kluczowych mechanizmów kontrolnych .....	14
DZIAŁ VII – System raportowania.....	17
DZIAŁ VIII – Audyt wewnętrzny .....	19
DZIAŁ IX – Postanowienia końcowe .....	20

# DZIAŁ I

## Rozdział 1 - Postanowienia ogólne

### §1

1. Niniejsza procedura określa:
  - 1) organizację systemu kontroli wewnętrznej,
  - 2) działanie funkcji kontroli,
  - 3) ogólne zasady zapewnienia zgodności,
  - 4) zadania Banku związane z funkcją audytu wewnętrznego.
2. Bank jest Uczestnikiem Systemu Ochrony SGB, w związku z tym w system kontroli wewnętrznej są wpisane mechanizmy określone w Umowie Systemu, w szczególności komórka audytu wewnętrznego - stanowiąca trzecią linię obrony w Banku - umiejscowioną w Spółdzielni.
3. Bank, określając poszczególne elementy modelu kontroli wewnętrznej, stosuje zasadę proporcjonalności, uwzględniając wielkość Banku mierzoną sumą bilansową oraz wielkością aktywów, a także profilem określonym w strategii zarządzania Bankiem i apetytem na ryzyko.
4. Niniejsza procedura – wraz z jej poszczególnymi elementami, podlega formalnemu przeglądowi i zatwierdzeniu przez Zarząd i Radę Nadzorczą, co najmniej raz w roku.
5. Właścicielem procedury są jednostki stanowiące element drugiej linii obrony (Komórka sprawozdawczości i ryzyka, stanowisko ds. monitoringu i windykacji, stanowisko ds. samorządu, kadr i zgodności i Stanowiska Analiz Kredytowych.).

### §2

Najważniejsze regulacje zewnętrzne i wewnętrzne, będące podstawą opracowania niniejszej procedury, to:

- 1) dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26.06.2013 r. *w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi (CRD IV)*;
- 2) ustawa Prawo bankowe;
- 3) ustawa z dnia 7 grudnia 2000 roku *o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających ( Dz. U. z 2015r. poz.2170 z późn. zm.)*
- 4) ustawa z dnia 11 marca 2016 r. o zmianie ustawy o Bankowym Funduszu Gwarancyjnym;
- 5) Rozporządzenie Ministra Rozwoju i Finansów z dnia 24.03 2017 roku *w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w bankach (D.U. z dnia 24.03.2017r. poz. 637)*;
- 6) Rekomendacja H Komisji Nadzoru Finansowego dotycząca systemu kontroli wewnętrznej w bankach;
- 7) Umowa Systemu Ochrony SGB;
- 8) Strategia na lata 2016-2020 zwana dalej Strategią;
- 9) Strategia zarządzania ryzykiem w Banku Spółdzielczym w Prabutach.

### §3

W dalszej treści użyte są następujące skróty i pojęcia, które oznaczają:

- 1) Bank – Bank Spółdzielczy w Prabutach;
- 2) Rada Nadzorcza – Rada Nadzorcza Banku;
- 3) Zarząd – Zarząd Banku;
- 4) Bank Zrzeszający – SGB-Bank S.A. w Poznaniu;

- 5) Spółdzielnia – jednostka zarządzająca Systemem Ochrony SGB;
- 6) Umowa/Umowa Systemu – Umowa Systemu Ochrony SGB;
- 7) funkcja kontroli – element systemu kontroli wewnętrznej, na który składają się wszystkie mechanizmy kontrolne w procesach funkcjonujących w Banku, niezależne monitorowanie przestrzegania tych mechanizmów kontrolnych oraz raportowanie w ramach funkcji kontroli;
- 8) jednostka kontrolowana - należy przez to rozumieć Bank oraz jego jednostki organizacyjne (punkt kasowy), komórki organizacyjne lub poszczególne stanowiska pracy w ramach jednostek i komórek organizacyjnych Banku;
- 9) komórka audytu - komórka Spółdzielni wykonująca zadania związane z wykonywaniem audytu wewnętrznego w Systemie Ochrony;
- 10) kluczowy mechanizm kontrolny - mechanizm o kluczowym znaczeniu dla osiągnięcia danego celu ogólnego lub szczegółowego systemu kontroli wewnętrznej w danym procesie, bez przestrzegania/stosowania którego może zaistnieć nieakceptowane przez Bank ryzyko, że taki cel nie zostanie osiągnięty;
- 11) matryca funkcji kontroli – opis powiązania celów ogólnych i wyodrębnionych w ich ramach celów szczegółowych systemu kontroli wewnętrznej z procesami istotnymi funkcjonującymi w Banku oraz kluczowymi mechanizmami kontrolnymi i niezależnym monitorowaniem przestrzegania tych mechanizmów kontrolnych;
- 12) mechanizm kontrolny - wyróżnione w ramach funkcji kontroli, wszelkie działania lub rozwiązanie wykonywane i stosowane w ramach trzech linii obrony, w tym zwłaszcza w ramach pierwszej linii obrony, mające za zadanie zapewnienie osiągnięcia celów ogólnych lub szczegółowych systemu kontroli wewnętrznej;
- 13) monitorowanie pionowe – niezależne monitorowanie przez drugą linię obrony (weryfikacja bieżąca lub testowanie) przestrzegania mechanizmów kontrolnych w ramach pierwszej linii obrony;
- 14) monitorowanie poziome – niezależne monitorowanie w ramach danej linii obrony (weryfikacja bieżąca lub testowanie) przestrzegania mechanizmów kontrolnych;
- 15) proces – zbiór wszelkich wzajemnie powiązanych ze sobą czynności wykonywanych przez jednostki, komórki, stanowiska organizacyjne banku oraz jego podmioty zależne, których realizacja jest niezbędna do uzyskania określonego rezultatu (np. udzielenie kredytu, sprzedaż wierzytelności, zaksięgowanie transakcji określonego rodzaju, sporządzanie sprawozdania finansowego). W ramach procesów wykonywane są operacje, transakcje oraz inne czynności niezbędne do uzyskania określonego rezultatu;
- 16) dokument testowy – dokument zawierający ustalenia i wnioski po przeprowadzonym testowaniu wraz z uwzględnieniem kategorii stwierdzonych nieprawidłowości;
- 17) strona kontrolowana – należy przez to rozumieć pracownika Banku kierującego jednostką kontrolowaną (w przypadku badanych komórek lub wykonującego zadania w jednostce kontrolowanej (w przypadku badanych stanowisk pracy));
- 18) strona kontrolująca – należy przez to rozumieć pracowników Banku przeprowadzających kontrolę wewnętrzną;
- 19) 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. 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);
- 20) 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).

## Rozdział 2 – Model trzech linii (poziomów) obrony

### §4

1. Funkcjonujący w banku system zarządzania ryzykiem i system kontroli wewnętrznej są zorganizowane na trzech, niezależnych i wzajemnie uzupełniających się liniach obrony (poziomach).
2. Na pierwszą linię obrony składa się operacyjne zarządzanie ryzykiem powstałym w związku z działalnością prowadzoną przez Bank.
3. Zgodnie z obowiązującą w Banku strukturą organizacyjną, w ramach poziomu wymienionego w ust. 2:
  - 1) Komórka zarządzająca (komórka organizacyjna wykonująca zadania związane z utrzymywaniem bieżącej i krótkoterminowej płynności Banku tj. z-ca Głównego Księgowego);
  - 2) Stanowiska kredytów;
  - 3) Stanowiska obsługi kasowo-depozytowej;
  - 4) Stanowiska ds. księgowości.
4. Na drugą linię obrony składa się zarządzanie ryzykiem przez pracowników na specjalnie powołanych do tego stanowiskach lub w komórkach organizacyjnych, niezależnie od operacyjnego zarządzania ryzykiem na pierwszym poziomie:
  - 1) Komórka ds. sprawozdawczości i ryzyka (monitorująca ryzyko z wyjątkiem indywidualnego ryzyka kredytowego),
  - 2) Stanowisko ds. Monitoringu i Windykacji (monitorujące indywidualne ryzyko kredytowe),
  - 3) Stanowisko ds. samorządu, kadr i zgodności (wykonujące zadania komórki ds. zgodności)
  - 4) Stanowiska analiz kredytowych.Do przykładowych mechanizmów kontrolnych drugiej linii obrony należą np:
  - 1) monitorowanie terminowości obsługi kredytów przez Stanowisko ds. monitoringu i windykacji (kontrola pionowa, niezależna, weryfikacja bieżąca); (ten mechanizm jest następnie testowany na próbie w ramach niezależnej pionowej kontroli przez III linię (komórkę audytu wewnętrznego),
  - 2) monitorowanie przestrzegania limitów przez Komórkę ds. sprawozdawczości i ryzyka (kontrola pionowa, niezależna, weryfikacja bieżąca); (ten mechanizm jest następnie testowany w ramach niezależnej pionowej kontroli na próbie np. raportów z przestrzegania limitów przez Stanowisko ds. samorządu, kadr i zgodności).
  - 3) kontrola jakości uruchomionych kredytów wykonywana przez Stanowisko ds. samorządu, kadr i zgodności obejmująca próbę uruchomień (kontrola pionowa, niezależna, testowanie) np. z ostatniego miesiąca (jakość, kompletność dokumentów, poprawność danych, itd.).
5. Trzecią linię obrony stanowi audyt wewnętrzny realizowany przez Spółdzielczy System Ochrony SGB<sup>1</sup>.
6. Na wszystkich trzech poziomach, w ramach systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, pracownicy Banku w ramach realizowanych czynności

---

<sup>1</sup> Departament Audytu Spółdzielczego Systemu Ochrony SGB

odpowiednio stosują mechanizmy kontrolne lub niezależnie monitorują (poziomo lub pionowo) przestrzeganie mechanizmów kontrolnych.

## §5

1. Pierwsza linia obrony odpowiedzialna jest m.in. za projektowanie i zapewnienie przestrzegania mechanizmów kontrolnych, w szczególności w procesach biznesowych funkcjonujących w Banku oraz zgodności postępowania z regulacjami.
2. Druga linia obrony odpowiedzialna jest w szczególności za:
  - 1) monitorowanie bieżące przyjętych mechanizmów kontrolnych,
  - 2) przeprowadzanie pionowych testów mechanizmów kontrolnych,
  - 3) ocenę adekwatności i skuteczności mechanizmów kontrolnych,
  - 4) matrycę funkcji kontroli,
  - 5) prowadzenie rejestru nieprawidłowości znaczących i krytycznych,
  - 6) raportowanie znaczących i krytycznych nieprawidłowości.
3. Trzecia linia obrony odpowiedzialna jest za badanie oraz ocenę adekwatności i skuteczności mechanizmów kontroli i niezależnego monitorowania ich przestrzegania odpowiednio w ramach pierwszej i drugiej linii obrony, zarówno w odniesieniu do systemu zarządzania ryzykiem, jak i systemu kontroli wewnętrznej.
4. Celem dokonania oceny, o której mowa w pkt. 3, komórka audytu wewnętrznego w ramach badań audytowych, bierze pod uwagę w szczególności wyniki oraz skuteczność i adekwatność weryfikacji bieżącej i testowania przestrzegania mechanizmów kontrolnych pierwszej i drugiej linii obrony.

## §6

1. W Banku zapewniona jest niezależność monitorowania pionowego poprzez jednoznaczne wyodrębnienie linii obrony oraz niezależność monitorowania poziomego poprzez rozdzielanie zadań dotyczących stosowania danego mechanizmu kontrolnego i niezależnego monitorowania jego przestrzegania w ramach danej linii.
2. Za monitorowanie poziome (weryfikacja bieżąca, testowanie) w ramach danej linii odpowiedzialni są wyznaczeni pracownicy, w tym kierownicy komórek organizacyjnych.
3. Za monitorowanie pionowe pierwszej linii obrony przez drugą linię obrony odpowiada Stanowisko ds. samorządu, kadr i zgodności (komórka ds. zgodności).

## **Rozdział 3 – Podział obowiązków**

### §7

#### Rola i zadania Rady Nadzorczej

1. Rada Nadzorcza sprawuje nadzór nad wprowadzeniem i zapewnieniem funkcjonowania adekwatnego systemu kontroli wewnętrznej oraz odpowiedzialna jest za monitorowanie jego skuteczności.
2. Nadzór Rady Nadzorczej nad funkcjonowaniem systemu kontroli wewnętrznej obejmuje m.in.:
  - 1) akceptowanie zasad funkcjonowania systemu kontroli wewnętrznej, w tym matrycy funkcji kontroli,
  - 2) coroczną ocenę adekwatności i skuteczności systemu kontroli wewnętrznej, w tym funkcji kontroli, komórki do spraw zgodności oraz wyników audytu przeprowadzonego przez komórkę audytu wewnętrznego,

- 3) ocenę efektów działań podjętych w celu usunięcia stwierdzonych nieprawidłowości w funkcjonowaniu mechanizmów kontrolnych,
- 4) zatwierdzenie zasad kategoryzacji nieprawidłowości wykrytych przez system kontroli wewnętrznej,
- 5) zatwierdzenie kryteriów adekwatności i skuteczności systemu kontroli wewnętrznej.

## §8

### Rola i zadania Zarządu Banku

1. Zarząd, w ramach trzech linii obrony, odpowiada za zaprojektowanie, wprowadzenie oraz zapewnienie we wszystkich komórkach/stanowiskach organizacyjnych Banku, funkcjonowania adekwatnego i skutecznego systemu kontroli wewnętrznej, który obejmuje funkcję kontroli i komórkę do spraw zgodności.
1. Do zadań Zarządu, należy w szczególności:
  - 1) ustanowienie, w ramach trzech linii obrony, kryteriów adekwatności i skuteczności systemu kontroli wewnętrznej,
  - 2) zapewnienie ciągłości i skuteczności działania systemu kontroli wewnętrznej, a także właściwej współpracy wszystkich pracowników Banku w ramach funkcji kontroli z komórką do spraw zgodności i komórką audytu wewnętrznego oraz dostępu osobom wykonującym czynności kontrolne/czynności audytowe do niezbędnych dokumentów źródłowych, w tym zawierających informacje poufne,
  - 3) określenie rodzaju działań podejmowanych w celu usunięcia nieprawidłowości wykrytych przez system kontroli wewnętrznej, w tym środki naprawcze i dyscyplinujące,
  - 4) sporządzanie okresowej (nie rzadziej niż raz w roku) informacji dla Rady Nadzorczej o sposobie wypełniania zadań przez pracowników Banku w ramach funkcji kontroli oraz komórki do spraw zgodności ze szczególnym uwzględnieniem:
    - adekwatności i skuteczności systemu kontroli wewnętrznej w zapewnieniu osiągnięcia każdego z celów systemu kontroli wewnętrznej,
    - skali i charakterze nieprawidłowości znaczących i krytycznych oraz najważniejszych działań zmierzających do usunięcia tych nieprawidłowości, w tym o podjętych środkach naprawczych i dyscyplinujących,
    - zapewnienia niezależności komórce do spraw zgodności,
    - zapewnienia środków finansowych niezbędnych do skutecznego wykonywania przez pracowników komórki zgodności oraz do systematycznego podnoszenia kwalifikacji oraz zdobywania doświadczenia i umiejętności przez pracowników tej komórki,
  - 5) zatwierdzanie listy istotnych procesów wyodrębnionych przez Bank oraz ich powiązanie z celami ogólnymi i szczegółowymi systemu kontroli wewnętrznej,
  - 6) zapewnienie dokonywania regularnego przeglądu wszystkich procesów funkcjonujących w Banku pod kątem ich istotności,
  - 7) zatwierdzenie zasad kategoryzacji nieprawidłowości wykrytych przez system kontroli wewnętrznej,
  - 8) zapewnienie niezależnego monitorowania przestrzegania mechanizmów kontrolnych poprzez określenie odpowiedniego jego zakresu i kryteriów,
  - 9) wyznaczenie komórki organizacyjnej/stanowiska odpowiedzialnej za zadania związane z prowadzeniem matrycy funkcji kontroli, określenie formy udokumentowania przeprowadzonego przeglądu i oceny efektywności wewnętrznych mechanizmów kontrolnych oraz wniosków wynikających z tych przeglądów,

- 10) określenie trybu przekazania wewnątrz Banku raportu pokontrolnego/raportu, w celu podjęcia działań służących usunięciu stwierdzonych nieprawidłowości mechanizmów kontroli oraz sposobu kontroli skorygowania tych nieprawidłowości.

## §9

### Rola i zadania stanowiska ds. samorządu kadr i zgodności

1. W Banku, w pionie Prezesa Zarządu, działa Stanowisko ds. samorządu, kadr i zgodności odpowiedzialne za wykonywanie zadań związanych z niezależnym monitorowaniem pionowym.
2. Do zadań tej komórki należy m.in.:
  - 1) przeprowadzanie pionowych testów przestrzegania kluczowych mechanizmów kontrolnych,
  - 2) ocena adekwatności i skuteczności kluczowych mechanizmów kontrolnych,
  - 3) prowadzenie rejestru nieprawidłowości istotnych i krytycznych,
  - 4) raportowanie o przestrzeganiu kluczowych mechanizmów kontrolnych, obejmujące co najmniej zestawienie wykrytych nieprawidłowości znaczących i krytycznych,
  - 5) administrowanie matrycą funkcji kontroli, w tym pozyskiwanie informacji niezbędnych do przygotowania i aktualizacji matrycy.
3. Stanowisko ds. samorządu, kadr i zgodności odpowiedzialne jest za ponadto za identyfikację, ocenę, kontrolę i monitorowanie ryzyka braku zgodności działalności Banku z przepisami prawa, regulacjami wewnętrznymi i standardami rynkowymi (w szczególności rekomendacjami UKNF nie związanymi z zarządzaniem ryzykiem).
4. W ramach funkcji kontroli, stanowisko ds. samorządu, kadr i zgodności odpowiedzialne jest m.in. za zapewnienie zgodności poprzez:
  - 1) weryfikację bieżącą pionową, w ramach drugiej linii obrony,
  - 2) testowanie pionowe przestrzegania kluczowych mechanizmów kontrolnych, zapewniających osiągnięcie zgodności działania Banku z przepisami prawa, regulacjami wewnętrznymi i standardami rynkowymi.
5. Proces zarządzania ryzykiem braku zgodności określony został w „Zasadach zarządzania ryzykiem braku zgodności w Banku Spółdzielczym w Prabutach”.

## §10

### Rola i zadania komórki audytu wewnętrznego

1. Komórka audytu wewnętrznego - komórka Spółdzielni wykonująca zadania związane z wykonywaniem audytu wewnętrznego w Systemie Ochrony.
2. Zasady wykonywania audytu wewnętrznego przez komórkę audytu wewnętrznego Spółdzielczego Systemu Ochrony SGB określone zostały w Załączniku nr 4 i 4a do Umowy Systemu Ochrony.

## §11

### Rola i zadania kadry kierowniczej

Kierownicy jednostek i komórek organizacyjnych Banku, wypełniając swoje obowiązki, wprowadzają w życie przyjęte przez Zarząd wewnętrzne strategie i procedury dotyczące zarządzania ryzykiem, a przede wszystkim:



- 1) odpowiadają za wdrożenie odpowiednich mechanizmów kontrolnych,
- 2) monitorują prawidłowość przestrzegania mechanizmów kontrolnych.

## DZIAŁ II – Funkcja kontroli

Na funkcję kontroli składają się wszystkie mechanizmy kontrolne w procesach funkcjonujących w Banku, niezależne monitorowanie przestrzegania mechanizmów kontrolnych oraz raportowanie w ramach funkcji kontroli.

### Rozdział 1 – Cele systemu kontroli wewnętrznej

#### §12

1. Celem ogólnym systemu kontroli wewnętrznej jest zapewnienie:
  - 1) skuteczności i efektywności działania Banku,
  - 2) wiarygodności sprawozdawczości finansowej,
  - 3) przestrzegania zasad zarządzania ryzykiem w Banku,
  - 4) zgodności działania Banku z przepisami prawa, regulacjami wewnętrznymi i standardami rynkowymi.

#### §13

1. W ramach celów ogólnych systemu kontroli wewnętrznej Bank wyodrębnia cele szczegółowe, do których zalicza się m.in.:
  - 1) wykrycie błędów i nadużyć (np. przy akceptacji na drugą rękę) – (miernik: akceptowalny poziom – „0” błędów krytycznych, „0” nadużyć),
  - 2) ochrona majątku (kontrola bezpieczeństwa, gotówkowe) – ( miernik: „0” błędów; max. dopuszczalny poziom niezgodności kasowych- 0,00 zł.),
  - 3) wiarygodność i integralność informacji (np. kontrola jakości i kompletności dokumentów, jakość danych w systemie) – (miernik: „0” błędów krytycznych),
  - 4) terminowość realizacji zadań (np. brak reklamacji, dotrzymanie terminów; max. długość podejmowania decyzji kredytowych - zgodnie z procedurami ),
  - 5) skuteczność i wydajność (np. windykacji),
  - 6) zgodność z prawem i regulacjami (mierniki „0” błędów krytycznych; ilość reklamacji- „0” reklamacji pozakartowych, sprawy sądowe – „0”),
  - 7) dostępność systemów i aplikacji (np. skuteczność planów awaryjnych, mała awaryjność) – ( miernik: max. czas niedostępności systemu- 15 min., usług elektronicznych- 15 min., skargi i reklamacje – „0”; „0” błędów krytycznych),
  - 8) poufność informacji i danych ( miernik: „0” błędów krytycznych np. „wypłynięcia danych”, skargi i reklamacje „0”),
  - 9) adekwatność informacji zarządczej (np. informacja kompletna, rzetelna, na czas, miernik: brak błędów krytycznych w wyniku kontroli pionowych),
  - 10) poprawność prezentacji i ujęcia sprawozdań finansowych (np. ilość błędów istotnych- „0”, „zero” krytycznych),
  - 11) racjonalne wykorzystywanie zasobów ( C/I + mierniki efektywnościowe; mierniki na poziomie określonym przez Zarząd w procedurach),
  - 12) zapewnienie realizacji celów biznesowych (np. kluczowych celów określonych w procesach kredytowych lub innych istotnych sprzedażowo produktach; raporty zarządcze o realizacji celów, planów biznesowych; miernik: ocena jakości i kompletności oraz terminowości przez testowanie pionowe).

## §14

1. Każdy z procesów uznawany przez Bank za istotny jest powiązany z celami ogólnymi i szczegółowymi systemu kontroli wewnętrznej.
2. Bank wyodrębnia procesy uznane za istotne w oparciu o przyjęte kryteria wyboru z uwzględnieniem Strategii działania Banku, modelu biznesowego, strategii zarządzania ryzykiem i apetytu na ryzyko oraz wpływu danego procesu na wynik finansowy i adekwatność kapitałową.
3. Zgodnie z Rekomendacją M KNF Bank posiada dokumentację określającą jakiego rodzaju procesy występują w Banku, kto jest ich właścicielami oraz które z tych procesów Bank uznaje za kluczowe/istotne dla realizacji Strategii Banku, a które uznaje za krytyczne z punktu widzenia zachowania ciągłości działania. Wykaz procesów kluczowych i podprocesów stanowi załącznik nr 1 do niniejszej procedury.

## Rozdział 2 – Mechanizmy kontrolne

### §15

1. Mechanizmy kontrolne przyjęte w Banku wbudowane są w funkcjonujące w Banku procesy, czynności, w codzienną działalność operacyjną Banku.
2. Proces projektowania, zatwierdzania i wprowadzania w Banku mechanizmów kontrolnych jest odpowiednio udokumentowany i umożliwia przypisanie komórkom organizacyjnym odpowiedzialności za realizację zadań w poszczególnych etapach tego procesu.
3. Mechanizmy kontrolne przyjęte na poziomie wszystkich linii obrony spełniają rolę:
  - 1) *prewencyjną – zapobieganie nieprawidłowościom (np. zasady kontroli dostępu do systemu, niektóre kontrole automatyczne-aplikacyjne, Komitet Zarządzania Ryzykami),*
  - 2) *detekcyjną – wykrywanie nieprawidłowości (np. inwentaryzacja, kontrole kasowe, kontrole uruchomień kredytów, działania komórki monitorującej ryzyko portfelowe),*
  - 3) *korekcyjną – korygowanie nieprawidłowości (np. automatyczna walidacja pól w systemach).*
4. *W Banku stosuje się mechanizmy kontrolne:*
  - 1) *automatyczne (wbudowane w systemy informatyczne, najczęściej wymuszające lub uniemożliwiające pewne działania np. wymuszenie właściwej budowy hasła dostępu),*
  - 2) *półautomatyczne (np. monitorowanie limitów, wskaźników, weryfikacja danych),*
  - 3) *manualne (np. podział obowiązków, autoryzacja formalna na „drugą rękę”, uzgodnienia danych i inwentaryzacja, weryfikacja i analiza danych).*

Wszystkie mechanizmy znajdują odzwierciedlenie w procedurach różnego szczebla – zarówno politykach, jak i procedurach operacyjnych stosowanych przez pracowników niższego szczebla. Tym samym stanowią kluczowy element definiujący pożądane zachowania w ramach pierwszej i drugiej linii obrony. Stosowanie zapisów procedur w praktyce jest monitorowane w ramach testów pionowych i poziomych.

Poniżej tabela zawiera przykłady mechanizmów kontrolnych:

Lp.	Mechanizm kontrolny	Rodzaj mechanizmu
1.	Podział zadań, powierzenie odpowiednich funkcji (np. ABI, ASI), zakresy czynności i obowiązków, w tym: <ul style="list-style-type: none"><li>• kompetencje i odpowiedzialności,</li><li>• upoważnienia i pełnomocnictwa,</li></ul>	Manualny, półautomatyczny

	<ul style="list-style-type: none"> <li>• system zastępstw,</li> <li>• sprawowany nadzór przez przełożonego;</li> </ul>	
2.	<p>System obiegu informacji i raportowania, w tym:</p> <ul style="list-style-type: none"> <li>• zapewnienie dostępu do informacji w terminie i zakresie właściwym do wykonywania zadań,</li> <li>• raportowanie wykonania zadań do bezpośredniego przełożonego/dla Zarządu/Rady Nadzorczej,</li> <li>• porównywanie osiągniętych wyników z zamierzonymi celami;</li> </ul>	Manulany, półautomatyczny
3.	<p>Uzgadniania danych tzw. rekonyliacja i weryfikacja danych, w tym m.in.:</p> <ul style="list-style-type: none"> <li>• okresowe uzgadnianie, takie jak porównywanie dokumentów źródłowych transakcji z zestawieniem sald i obrotów,</li> <li>• weryfikacja szczegółowych transakcji i czynności, a także przyjmowanych założeń i wyników metod stosowanych przez Bank do zarządzania ryzykiem;</li> </ul>	Manulany, półautomatyczny, automatyczny
4.	<p>Zasad komisyjności „czworga oczu”, akceptacja na drugą rękę”, w tym m.in.:</p> <ul style="list-style-type: none"> <li>• realizowanie czynności przy współdziałaniu co najmniej dwóch osób,</li> <li>• komisje inwentaryzacyjne, spisowe,</li> <li>• rejestracja i autoryzacja dowodów księgowych lub transakcji;</li> </ul>	Manualny, półautomatyczny, automatycznych
5.	<p>System limitów i ograniczeń, w tym m.in.:</p> <ul style="list-style-type: none"> <li>• stosowanie ograniczeń czasowych dla rejestracji operacji, spłaty zobowiązania</li> <li>• monitorowanie wszelkiego rodzaju limitów ostrożnościowych</li> </ul>	Manulany, półautomatyczny,
6.	<p>Mechanizmy dostępu fizycznego (strefy wydzielone, zamki, kody dostępu, zabezpieczenia przed pożarem, zalaniem) oraz zabezpieczenia teleinformatyczne, w tym m.in.:</p> <ul style="list-style-type: none"> <li>• zakazy i ograniczenia dostępu fizycznego pracowników do pomieszczeń, systemów i danych, internetu,</li> <li>• nagrywanie rozmów telefonicznych,</li> <li>• zabezpieczenie gotówki, papierów wartościowych;</li> </ul>	Automatyczny, półautomatyczny, manulany
7.	<p>Inwentaryzacja i spisy z natury, w tym m.in.:</p> <ul style="list-style-type: none"> <li>• porównywanie zgodności stanu fizycznego/rzeczywistego zasobów ze stanem zapisów w księgach rachunkowych, rejestrach,</li> <li>• inwentaryzacja rzeczowych składników majątku,</li> <li>• dzienne uzgadnianie stanu wartości gotówki;</li> </ul>	Manualny półautomatyczny

8.	Tworzenie kopii zapasowych oraz ich testowanie	Automatyczny półautomatyczny
9.	Plany awaryjne, plany ciągłości działania oraz ich testowanie.	Manulany, półautomatyczny,

### §16

1. Jednym z mechanizmów kontrolnych jest ich niezależne monitorowanie (poziome i pionowe). Bank posiada mechanizmy kontrolne (tabela powyżej), a kluczowe z nich niezależnie monitoruje - ich skuteczność – poprzez testy pionowe lub testy poziome – lub jedno i drugie.
2. Im bardziej kluczowy jest dany mechanizm kontrolny w procesie uznanym za istotny, tym częściej i skuteczniej (na większej próbie) jest przedmiotem monitorowania pionowego.

### §17

1. W ramach przyjętych mechanizmów kontrolnych dla procesów istotnych Bank dokonuje, na podstawie określonych kryteriów, wyboru kluczowych mechanizmów kontrolnych.
2. Kluczowe mechanizmy kontrolne przypisane są co najmniej procesem istotnym.
3. Każdy z kluczowych mechanizmów kontrolnych jest szczegółowo opisany, tj. wskazane jest m.in.:
  - 1) kto jest właścicielem procesu istotnego, do którego został mechanizm przypisany,
  - 2) kto projektuje mechanizm, a kto odpowiada za jego wdrożenie i funkcjonowanie,
  - 3) jakie działania są wykonywane w ramach funkcjonowania mechanizmu kontrolnego, aby zapewnić, że cele tego mechanizmu zostaną osiągnięte,
  - 4) kto wykonuje działania kontrolne,
  - 5) jaki jest cel realizowanych czynności kontrolnych,
  - 6) na jakim etapie procesu realizowana jest kontrola i jaki okres obejmuje.
4. Przy opisie kluczowego mechanizmu kontrolnego określone jest również:
  - 1) rodzaj mechanizmu (np. manualny, automatyczny),
  - 2) częstotliwość jego stosowania,
  - 3) procedura opisująca sposób działania mechanizmu.
5. Ocena przestrzegania kluczowych mechanizmów kontrolnych jest dokonywana z odpowiednią częstotliwością w ramach niezależnego monitorowania oraz badania przez trzecią linię obrony.
6. Bank prowadzi ewidencję kluczowych mechanizmów kontrolnych w matrycy, która stanowi załącznik nr 2 do niniejszej procedury.

## Rozdział 3 – Niezależne monitorowanie

### §18

1. Niezależne monitorowanie przestrzegania mechanizmów kontrolnych obejmuje weryfikację bieżącą i testowanie.
2. Bank dokonując wyboru rodzajów niezależnego monitorowania, w ramach monitorowania pionowego i poziomego, stosuje odpowiednio zasadę proporcjonalności pomiędzy weryfikacją bieżącą i testowaniem.

### §19

1. Niezależne monitorowanie przestrzegania mechanizmów kontrolnych jest wpisane we wszystkie procesy istotne funkcjonujące w Banku.
2. Pracownicy mają w jednoznaczny sposób przypisane w regulacjach wewnętrznych/kartach obowiązków odpowiedzialność związaną z monitorowaniem pionowym i poziomym oraz posiadają odpowiednie kwalifikacje, doświadczenie i umiejętności w zakresie związanym z realizacją tych zadań.
3. Monitorowanie przestrzegania mechanizmów kontrolnych obejmuje weryfikację bieżącą i testowanie w ramach monitorowania pionowego i poziomego z uwzględnieniem:
  - celów systemu kontroli wewnętrznej,
  - złożoności procesów, w tym zwłaszcza procesów istotnych,
  - liczby, rodzaju i stopnia złożoności mechanizmów kontrolnych,
  - ryzyka zaistnienia nieprawidłowości,
  - zasobów poszczególnych linii obrony, w tym kwalifikacji, doświadczenia i umiejętności pracowników tych linii,
  - zasady proporcjonalności.

## §20

1. Weryfikacja bieżąca przeprowadzana jest przed rozpoczęciem lub w trakcie czynności wykonywanych w ramach danego procesu.
2. Weryfikacja bieżąca jest przeprowadzana (w szczególności w ramach pierwszej linii obrony) przez:
  - 1) przełożonego w ramach wykonywania nadzoru służbowego (kontrola bieżąca),
  - 2) innego pracownika tej samej komórki w ramach podziału obowiązków lub innej komórki organizacyjnej tej samej linii obrony (tzw. kontrola na drugą rękę – monitorowanie poziome).

## §21

1. Testowanie przeprowadzana jest na wybranej próbie testowej, po zakończeniu czynności wykonywanych w ramach danego procesu lub poszczególnych etapów tych czynności.
2. Testowanie poziome komórki organizacyjnej w ramach tej samej linii obrony polega na testowaniu, co najmniej przestrzegania mechanizmów kontrolnych (np. przełożony testuje próbę transakcji swoich pracowników z częstotliwością określoną w macyzy kontroli).
3. Testowanie pionowe – testowanie przez Stanowisko ds. samorządu, kadr i zgodności przestrzegania kluczowych mechanizmów kontrolnych, w szczególności testowanie pierwszej linii obrony w przypadku procesów istotnych (np. monitoring niezależny polegający na sprawdzeniu czy przełożony faktycznie testuje próbę transakcji swoich pracowników zgodnie z macyzyą kontroli poprzez sprawdzenie udokumentowania oraz retesty na próbie).

## §22

1. W ramach niezależnego monitorowania ocenie podlegają m.in.:
  - 1) poziom ryzyka i sposób jego monitorowania,
  - 2) prawidłowość, terminowość i skuteczność realizacji zadań,
  - 3) przestrzeganie zasad wynikających z wewnętrznych i zewnętrznych aktów prawnych,
  - 4) bezpieczeństwo operacji bankowych,
  - 5) przestrzeganie kompetencji,
  - 6) sprawność organizacji,
  - 7) poprawność i kompletność dokumentów bankowych,
  - 8) rzetelność i prawidłowość danych księgowych,
  - 9) rzetelność i kompletność informacji,

- 10) zabezpieczenie mienia.
2. Kryterium oceny może być stwierdzenie błędów znaczących i krytycznych. Każdy niezależny monitoring dotyczący mechanizmów kontrolnych w procesach istotnych musi być udokumentowany, kończyć się raportem/informacją dla Zarządu lub być elementem większego raportu dla Zarządu zawierającym wnioski o stwierdzonych błędach oraz rekomendacji ich naprawy.

## **DZIAŁ IV – Matryca funkcji kontroli**

### **§23**

1. Matryca kontroli jest podstawowym narzędziem do operacyjnego zarządzania systemem kontroli wewnętrznej.
2. Matryca kontroli zawiera:
  - 1) listę procesów istotnych (o których mowa w §15 niniejszej procedury) wybranych w oparciu o adekwatne kryteria zatwierdzone przez Zarząd,
  - 2) cele kontroli przypisane poszczególnym procesom istotnym w podziale na cele ogólne i szczegółowe,
  - 3) kluczowe mechanizmy kontrolne wraz z ich opisem,
  - 4) zasady funkcjonowania poszczególnych mechanizmów kontrolnych,
  - 5) sposoby niezależnego monitorowania mechanizmów kontrolnych (wraz z zasadami dokumentowania i raportowania),
  - 6) zasady raportowania o istotnych i krytycznych nieprawidłowościach oraz sposobach ich naprawy.
3. Bank przygotowuje matrycę kontroli, która podlega zatwierdzeniu przez Zarząd.
4. Właścicielem matrycy kontroli jest Stanowisko ds. samorządu, kadr i zgodności. Jednostka jest odpowiedzialna za koordynację zadań związanych z przygotowaniem matrycy, jej fizyczne przygotowanie oraz przechowywanie, a także monitorowanie okresowych przeglądów.
5. Pozostałe jednostki są zobowiązane do aktywnego uczestnictwa w tworzeniu matrycy oraz są odpowiedzialne za zawartość merytoryczną opisów związanych z procesami, którymi zarządzają.
6. Matryca jest przedmiotem przeglądu i aktualizacji co najmniej raz w roku, a wszelkie zmiany podlegają zatwierdzeniu przez Zarząd.

### **§24**

1. W celu przygotowania matrycy Bank określa procesy istotne (o których mowa w §15 niniejszej procedury) dla procesów biznesowych. Bank uwzględnia proces zarządzania systemami informatycznymi w matrycy funkcji kontroli.
2. Bank posiada dokumentację wewnętrzną opisującą procesy, a także regularnie ocenia ich adekwatność, uwzględniając aktualność oraz zakres dystrybucji i wykorzystanie.
3. Realizowane przez Bank procesy są zinwentaryzowane i posiadają przypisanych właścicieli oraz są opisane na poziomie szczególności odpowiadającym istotności danego procesu dla Banku.
4. Zdefiniowane procesy są co do zasady, takie same jak wykorzystywane do zarządzania ryzykiem operacyjnym.

### **§25**

Dla wyodrębnionych procesów istotnych Bank definiuje:

- 1) cele kontroli – powiązując te cele zarówno z celami ogólnymi (Prawo bankowe) i celami szczegółowymi,
- 2) kluczowe mechanizmy kontrolne dla danego procesu (przy czym definiuje szczegółowo kluczowy mechanizmy oraz charakteryzuje jego rodzaj),
- 3) jak dane mechanizmy – ich adekwatność i skuteczność – będą kontrolowane poprzez testowanie poziome i/lub pionowe (niezależne monitorowanie) w ramach poszczególnych linii obrony,
- 4) sposób raportowania o wynikach kontroli, w tym w szczególności o stwierdzeniu wystąpienia nieprawidłowości o charakterze znaczącym i krytycznym.

Matryca kontroli stanowi załącznik nr 2 do procedury.

## **DZIAŁ V – Weryfikacja bieżąca kluczowych mechanizmów kontrolnych**

### **§26**

1. Weryfikacja bieżąca (poziom, pionowa) kluczowych mechanizmów kontrolnych przeprowadzana jest przez pracowników wskazanych w matrycy funkcji kontroli.
2. Sposób przeprowadzenia i dokumentowania weryfikacji bieżącej (poziomej, pionowej) oraz jej częstotliwość wynika z zapisów obowiązujących regulacji wewnętrznych obejmujących weryfikowane mechanizmy kontrolne (są nimi np. regulacje produktowe, uchwały kompetencyjne, regulaminy Komitetów).

## **DZIAŁ VI – Testowanie kluczowych mechanizmów kontrolnych**

### **Rozdział 1 – Planowanie testowani**

#### **§27**

1. Testowanie (poziome, pionowe) przeprowadzane jest przez kadrę kierowniczą (Kierownik Pionu ds. Handlowych, Z-ca Gł. Księgowego, Członkowie Zarządu. Testowania nie przeprowadza Kierownik Komórki ds. Sprawozdawczości i ryzyka z racji wykonywania czynności operacyjnych), Stanowisko ds. samorządu, kadr i zgodności lub osobę wyznaczoną, wynika z matrycy kontroli i ma charakter planowy.
2. Planowanie testowania opiera się na analizie ryzyka, przy uwzględnieniu w szczególności:
  - 1) specyfiki działania komórek organizacyjnych, w tym ilości i złożoności wykonywanych zadań,
  - 2) czynności i operacji, o znacznym ryzyku wystąpienia nieprawidłowości, a także możliwości popełnienia czynów, które mogą spowodować stratę dla Banku i/lub klientów,
  - 3) nowych rodzajów świadczonych usług lub nowo wprowadzonych produktów,
  - 4) stanu zatrudnienia,
  - 5) obszarów, w których stwierdzono nieprawidłowości, zwłaszcza o charakterze znaczącym i krytycznym w trakcie wcześniejszych testów (pionowych i poziomych),
  - 6) wyników audytów wewnętrznych i zewnętrznych,
  - 7) bezpieczeństwa systemów informatycznych.

3. Obszary zwiększonego ryzyka muszą być testowane regularnie i z większą częstotliwością.
4. Częstotliwość testowania musi zostać zwiększona, jeśli stwierdzono nieprawidłowości o charakterze znaczącym i krytycznym albo jeśli wprowadzono duże zmiany w odniesieniu do oferowanych produktów i usług, metodologii, pomiaru i monitorowania ryzyka, czy ogólnego profilu ryzyka w Banku.

#### §28

1. Plan testowania (poziomego i pionowego) opracowany jest na podstawie matrycy funkcji kontroli.
2. Plan testowania (poziomego i pionowego) określa temat testu oraz termin jego przeprowadzenia.
3. Plan testowania (poziomego i pionowego) sporządzany jest dla każdej komórki organizacyjnej Banku odrębnie.
4. Plan testowania stanowi załącznik nr 3 do niniejszej procedury.

### **Rozdział 2 – Przeprowadzenie testowania**

#### §29

Sposób testowania kluczowego mechanizmu kontrolnego określony jest indywidualnie dla każdego mechanizmu zgodnie z załącznikiem nr 4 do niniejszej procedury.

#### §30

W przypadku ujawnienia w trakcie testowania okoliczności mogących narazić Bank na straty i/lub noszących znamiona przestępstwa, strona kontrolująca bezzwłocznie zawiadamia o tym Prezesa Zarządu.

#### §31

Strona kontrolująca ma prawo, za zgodą Prezesa Zarządu, do niezbędnego rozszerzenia zakresu testowania, jeżeli w trakcie jego przeprowadzania zajdzie taka potrzeba.

### **Rozdział 3 – Postępowanie pokontrolne**

#### §32

1. Po zakończeniu testowania strona kontrolująca dokonuje wpisu w ewidencji testowania prowadzonej w Banku odrębnie dla poszczególnych jednostek organizacyjnych.
2. Wzór ewidencji testowania stanowi załącznik nr 5 do niniejszej procedury.

#### §33

1. Strona kontrolująca zobowiązana jest do przedstawienia wyników testowania, w tym:
  - 1) ustaleń z przeprowadzonego testu wraz z uwzględnieniem kategorii stwierdzonych nieprawidłowości,
  - 2) wniosków opartych na ustaleniach.
2. W przypadku stwierdzenia nieprawidłowości o charakterze znaczącym i krytycznym sposób raportowania regulują zapisy §42 niniejszej procedury.



### §34

1. Dokument testowy, o którym mowa w §29 niniejszej procedury wypełniany jest na bieżąco w trakcie przeprowadzania testu kluczowego mechanizmu kontrolnego.
2. Po zakończeniu testowania strona kontrolująca przedstawia wyniki w dokumencie testowym.
3. Strona kontrolująca uzgadnia dokument testowy ze stroną kontrolowaną.

### §35

1. Zalecenia pokontrolne w szczególności dla nieprawidłowości znaczących i krytycznych wydaje Prezes Zarządu.
2. Sposób naprawy pozostałych nieprawidłowości określa strona kontrolująca.
3. Dla każdego z zaleceń należy określić termin realizacji zalecenia wraz ze wskazaniem osoby odpowiedzialnej za jego realizację.
4. Monitorowanie stopnia realizacji zaleceń pokontrolnych przeprowadza wyodrębnione w strukturze organizacyjnej stanowisko, któremu powierzono testowanie (poziome/pionowe) oraz monitorowanie stopnia wykonania zaleceń pokontrolnych.

### §36

1. Za prawidłową i pełną realizację wniosków i wykonanie zaleceń pokontrolnych odpowiada strona kontrolowana.
2. Po upływie terminu realizacji zalecenia osoba odpowiedzialna za jego realizację zobowiązana jest do poinformowania strony kontrolującej o stopniu realizacji tego zalecenia.

### §37

1. Strona kontrolująca ma obowiązek sprawdzenia realizacji wykonania zaleceń przez stronę kontrolowaną najpóźniej w trakcie następnego testowania lub podczas odrębnego postępowania pokontrolnego. Informację o sprawdzeniu realizacji zaleceń strona kontrolująca umieszcza w dokumencie testowym sporządzonym po kolejnym testowaniu lub dokumencie testowym dotyczącym badania realizacji zaleceń.
2. Testowanie z zakresu realizacji zaleceń jest konieczne w sytuacji, gdy kategoria stwierdzonych nieprawidłowości jest znacząca lub krytyczna i ich wyeliminowanie powinno nastąpić jak najszybciej.
3. Weryfikacja realizacji zaleceń dla nieprawidłowości znaczących i krytycznych przeprowadzana jest na dokumencie testowym, o którym mowa w §29 niniejszej procedury.

### §38

Wszelkie zastrzeżenia strony kontrolowanej do wyników testowania rozstrzygane są w przypadku:

- 1) testowania poziomego z udziałem komórki do spraw zgodności,
- 2) testowania pionowego z udziałem bezpośredniego przełożonego strony kontrolowanej.

## DZIAŁ VII – System raportowania

### Rozdział 1 – Zasady kategoryzacji nieprawidłowości

#### §39

1. Bank określa kategorie nieprawidłowości wykrytych przez system kontroli wewnętrznej, biorąc pod uwagę ich negatywny wpływ na zapewnienie osiągnięcia określonych celów systemu kontroli wewnętrznej.
2. Nadanie odpowiedniej kategorii nieprawidłowości stwierdzonej, w ramach niezależnego monitorowania, polega na oszacowaniu poziomu ryzyka związanego z tą nieprawidłowością.
3. Oszacowany poziom ryzyka stanowi wypadkową prawdopodobieństwa jego wystąpienia oraz jego wpływu na sytuację Banku. Szacowane jest prawdopodobieństwo zmaterializowania się ryzyka związanego ze stwierdzoną nieprawidłowością w odniesieniu do okresu rocznego oraz określany jest wpływ stwierdzonej nieprawidłowości na sytuację Banku, tj.:
  - 1) wpływ finansowy - określa się wielkość wpływu stwierdzonej nieprawidłowości np. na poziom współczynników kapitałowych lub/i, tworzonych rezerw celowych/ odpisów utraty wartości lub/i, należności zagrożonych lub/i, norm płynności/LCR, wyniku finansowego lub/i, ryzyka stopy procentowej,
  - 2) wpływ operacyjny - należy określić wielkość wpływu stwierdzonej nieprawidłowości np. w odniesieniu do: ilości klientów Banku lub pracowników, jakości współpracy z podmiotami zewnętrznymi, wielkości okresu utraty kluczowych bądź niekluczowych systemów,
  - 3) wpływ reputacyjny - należy określić czy stwierdzona nieprawidłowość wpłynie na np. niekorzystny komentarz w mediach, formalną interwencję władz regulacyjnych, które może prowadzić do upomnienia i/lub kary pieniężnej, istotne niezgodności o charakterze compliance.
4. Zgodnie z poniższą matrycą dokonywana jest wycena ryzyka dotycząca danej nieprawidłowości, która jest podstawą nadania odpowiedniej kategorii nieprawidłowości.

#### WYCENA RYZYKA DLA NIEPRAWIDŁOŚCI

		PRAWDOPODOBIEŃSTWO			WPLYW		
		<b>Niskie</b>	Średnie	Wysokie	Wpływ finansowy	Wpływ operacyjny	Wpływ na reputację
Kategorie	<b>wysok</b>	UMIARKOWANE	PODWYŻSZONE	PODWYŻSZONE	pow. 5 tys. zł.	KRYTYCZNY	KRYTYCZNY
	<b>Średni</b>	NISKIE	UMIARKOWANE	UMIARKOWANE	od 500 zł. do 5 tys. zł.	ZNACZĄCY	ZNACZĄCY
	<b>Niski</b>	NISKIE	NISKIE	UMIARKOWANE	do 500 zł.	MAŁO ZNACZĄCY	MAŁO ZNACZĄCY

5. Poziomowi ryzyka przypisywana jest odpowiednia kategoria nieprawidłowości, wg poniższych zasad:

<b>Kategoria nieprawidłowości</b>	<b>Poziom ryzyka</b>
<b>KRYTYCZNA</b>	<b>Wysoki</b>
<b>ZNACZĄCA</b>	<b>Podwyższony</b>
<b>MAŁO ZNACZĄCA</b>	<b>Umiarkowany</b>
<b>NIEZNACZĄCA</b>	<b>Niski</b>

6. W Banku prowadzony jest rejestr wszystkich nieprawidłowości znaczących i krytycznych, którego wzór stanowi załącznik nr 7 do niniejszej procedury.
7. Za prowadzenie rejestru odpowiedzialna jest Stanowisko ds. samorządu, kadr i zgodności.

## **Rozdział 2 – Raportowanie**

### **§40**

1. Kadra kierownicza, Stanowisko ds. samorządu, kadr i zgodności lub osoby wyznaczone w poleceniu przeprowadzenia testu nieplanowego, w okresach kwartalnych przygotowują sprawozdanie z testowania.
2. Wzór sprawozdania z testowania stanowi załącznik nr 6 do niniejszej procedury.

### **§41**

1. Na podstawie informacji zawartych w sprawozdaniach, o których mowa w §40 ust.1 Stanowisko ds. samorządu, kadr i zgodności sporządza półroczne sprawozdanie o wynikach testowania pionowego i poziomego przestrzegania kluczowych mechanizmów kontrolnych z uwzględnieniem m.in. zestawienia wykrytych nieprawidłowości znaczących i krytycznych oraz informacji dotyczących efektów działań podjętych w celu usunięcia tych nieprawidłowości.
2. Sprawozdanie, o którym mowa w ust. 1, przekazywane jest Zarządowi i Radzie Nadzorczej w okresach półrocznych.

### **§42**

1. Wykryte w ramach pierwszej linii obrony nieprawidłowości znaczące lub krytyczne, są niezwłocznie raportowane do komórki organizacyjnej drugiej linii obrony, odpowiedzialnej za niezależne monitorowanie procesu, w ramach którego zaistniała dana nieprawidłowość znacząca lub krytyczna, a w przypadku nieprawidłowości krytycznych również do Zarządu Banku oraz komórki audytu wewnętrznego.
2. Wykryte w ramach drugiej linii obrony nieprawidłowości znaczące lub krytyczne, są niezwłocznie raportowane do Zarządu Banku i Rady Nadzorczej, a w przypadku nieprawidłowości krytycznych również do komórki audytu wewnętrznego.
3. Formą niezwłocznego raportowania może być np.: wysłanie wiadomości mailem, powiadomienie osobiste/telefoniczne.

### **§43**

1. Zgodnie z Umową Systemu Ochrony komórka audytu wewnętrznego przygotowuje syntetyczną informację o najistotniejszych nieprawidłowościach, stwierdzanych w trakcie audytów wewnętrznych i w okresach półrocznych przekazuje do Banku.
2. Bank wykorzystuje informacje, o którym mowa w ust. 1, w bieżącej pracy, w celu poprawy jakości wykonywanych usług i obniżenia poziomu ryzyka prowadzonej działalności.

## **DZIAŁ VIII – Audyt wewnętrzny**

### **§44**

1. Audyt wewnętrzny sprawowany jest przez komórkę audytu wewnętrznego Spółdzielni.
2. Planowanie i proces audytu wewnętrznego precyzują zapisy załącznika nr 4a do Umowy Systemu Ochrony oraz metodyki audytu.

### **§45**

1. Zakres badań audytowych jest:
  - 1) modyfikowany, w zależności od celu konkretnego audytu oraz analizy ryzyk środowiska kontrolnego,
  - 2) dostosowany do wyników oraz skuteczność i adekwatność weryfikacji bieżącej i testowania przestrzegania mechanizmów kontrolnych przez komórki organizacyjne w ramach pierwszej i drugiej linii obrony.

### **§46**

1. Wyniki audytu wewnętrznego przedstawione są w formie raportu, który otrzymują:
  - 1) Zarząd Spółdzielni,
  - 2) Zarząd Banku,
  - 3) Rada Nadzorcza Spółdzielni w przypadku audytów wewnętrznych, które zleciła.

### **§47**

1. W przypadku stwierdzenia, w wyniku audytu wewnętrznego, nieprawidłowości w działaniu Banku, Zarząd Spółdzielni wydaje zalecenia poaudytowe.
2. Bank zobowiązany jest do realizacji wydanych zaleceń poaudytowych.
3. Na podstawie wydanych zaleceń poaudytowych Bank opracowuje harmonogram realizacji przedmiotowych zaleceń i przekazuje go do komórki audytu wewnętrznego Spółdzielni, w terminie 15 dni roboczych od otrzymania zaleceń.
4. Harmonogram uznawany jest za przyjęty, jeżeli w terminie do 15 dni roboczych od daty otrzymania przez komórkę audytu wewnętrznego, nie zostaną do niego wniesione przez Zarząd Spółdzielni zastrzeżenia.

### **§48**

1. Za prawidłową i pełną realizację zaleceń poaudytowych odpowiada Zarząd Banku.
2. Bank przekazuje komórce audytu wewnętrznego informację o stopniu realizacji zaleceń poaudytowych oraz skutkach podjętych działań naprawczych.
3. W przypadku, gdy podjęte przez Bank działania nie doprowadziły do zrealizowania zaleceń w terminie określonym w harmonogramie realizacji zaleceń, Zarząd Banku

przekazuje do komórki audytu wewnętrznego pisemny, uzasadniony wniosek o przesunięcie terminu realizacji zaleceń, proponując nowy termin.

#### §49

Komórka audytu ma obowiązek weryfikacji stopnia realizacji zaleceń poaudytowych po upływie terminu realizacji zalecenia, a także w toku kolejnego audytu obejmującego analogiczny zakres podmiotowy i przedmiotowy lub audytu sprawdzającego dotyczącego badania realizacji zaleceń.

### **DZIAŁ IX – Postanowienia końcowe**

#### §50

Bank ogłasza w sposób ogólnie dostępny, w tym na stronie internetowej, opis systemu kontroli uwzględniający:

- 1) cele systemu kontroli wewnętrznej,
- 2) rolę Zarządu Banku i Rady Nadzorczej,
- 3) przyjęty schemat organizacji trzech linii obrony w ramach struktury organizacyjnej Banku,
- 4) funkcje kontroli,
- 5) umiejscowienie, zakres zadań, niezależność komórki do spraw zgodności,
- 6) zasady corocznej oceny skuteczności i adekwatności systemu kontroli wewnętrznej, dokonywanej przez Radę Nadzorczą.

#### §51

W Dziale V i VI niniejszej procedury opisany jest proces weryfikacji bieżącej i testowania dla kluczowych mechanizmów kontrolnych.

Zgodnie z zapisami §20 niniejszej procedury niezależne monitorowanie obejmuje również skuteczność działania pozostałych mechanizmów kontrolnych (niezdefiniowanych w matrycy jako kluczowe).

#### §52

Integralną częścią niniejszej procedury są załączniki od numeru 1- 7