Załącznik nr 2 do uchwały nr 33/2023 Zarządu z dnia 27 lutego 2023 r.

Raport ujawnieniowy dot. zasad zarządzania

Krajowa Izba Rozliczeniowa S.A.

Opis zasad zarządzania w Krajowej Izbie Rozliczeniowej S.A.
– informacja dla uczestników systemów płatności

Stan na 1 lutego 2023 r.

Krajowa Izba Rozliczeniowa S.A. (KIR) jest spółką akcyjną, której akcjonariuszami są: Narodowy Bank Polski, Santander Bank S.A., Powszechna Kasa Oszczędności Bank Polski S.A., mBank S.A., ING Bank Śląski S.A., Bank Polska Kasa Opieki S.A., Bank Millennium S.A., Bank Handlowy w Warszawie S.A., BNP Paribas Bank Polska S.A., Bank Polskiej Spółdzielczości S.A., SGB-Bank S.A. oraz Związek Banków Polskich.

Udział poszczególnych akcjonariuszy w kapitale zakładowym KIR został przedstawiony – również graficznie – pod adresem: https://www.kir.pl/o-nas/akcjonariat/.

Organami KIR są: Walne Zgromadzenie, Rada Nadzorcza i Zarząd.

Zgodnie ze Statutem Krajowej Izby Rozliczeniowej S.A., Rada Nadzorcza składa się z co najmniej 9 członków powoływanych po jednym – przez każdego z akcjonariuszy posiadających co najmniej 300 akcji. Prawo do powołania jednego członka Rady Nadzorczej przysługuje Narodowemu Bankowi Polskiemu niezależnie od jego uczestnictwa w akcjonariacie KIR. Członek Rady Nadzorczej powołany przez akcjonariusza może zostać odwołany jedynie przez tego akcjonariusza, a na jego miejsce akcjonariusz ten może powołać inną osobę. Na członka Rady Nadzorczej może być powołana przez akcjonariusza wyłącznie osoba będąca członkiem zarządu tego akcjonariusza lub pracownikiem tego akcjonariusza, legitymująca się odpowiednim wykształceniem oraz doświadczeniem w sektorze finansowym.

Rada Nadzorcza sprawuje stały nadzór nad działalnością KIR.

Aktualnie Rada Nadzorcza XI Kadencji składa się z 12 członków. Funkcję Przewodniczącego Rady Nadzorczej pełni członek Rady Nadzorczej powołany przez Narodowy Bank Polski.

W ramach swoich kompetencji Rada Nadzorcza powołała dwa stałe komitety, tj. Komitet do spraw Wynagrodzeń oraz Komitet Audytu i Ryzyka. Zgodnie z regulaminami tych komitetów, składają się one z co najmniej trzech członków, powoływanych przez Radę Nadzorczą uchwałą, spośród jej grona. Aktualnie w skład Komitetu do spraw Wynagrodzeń oraz Komitetu Audytu i Ryzyka wchodzi po 5 członków.

Zadaniem Komitetu do spraw Wynagrodzeń jest wsparcie Rady Nadzorczej w zakresie polityki wynagrodzeń członków Zarządu oraz innych warunków zatrudnienia członków Zarządu, a także wsparcie w zakresie powoływania i odwoływania członków Zarządu.

Zadaniem Komitetu Audytu i Ryzyka jest doradztwo na rzecz Rady Nadzorczej w kwestiach nadzoru nad właściwym stosowaniem w KIR zasad sprawozdawczości finansowej oraz współpraca z biegłymi rewidentami, a także doradztwo na rzecz Rady Nadzorczej w zakresie nadzoru nad funkcjonowaniem w KIR systemu zarządzania ryzykiem.

Zgodnie ze Statutem Krajowej Izby Rozliczeniowej S.A. Zarząd składa się z 3 do 6 członków, którzy są powoływani przez Radę Nadzorczą na wspólną, trzyletnią kadencję. Pracami Zarządu kieruje prezes Zarządu.

Zarząd kieruje bieżącą działalnością KIR i podejmuje decyzje we wszystkich sprawach nie zastrzeżonych dla Rady Nadzorczej i Walnego Zgromadzenia.

Zarząd realizuje swoje obowiązki informacyjne wobec Rady Nadzorczej zgodnie z ustawą z dnia 15 września 2000 r. – Kodeks spółek handlowych.

Aktualnie Zarząd składa się z trzech doświadczonych managerów, którzy w swojej karierze zawodowej pełnili istotne kierownicze funkcje w prestiżowych podmiotach rynku finansowego. Profil zawodowy członków Zarządu wiąże się z instytucjami finansowymi, w których pełnione funkcje zarządcze każdorazowo związane były z technologią informatyczną.

Działalność KIR realizowana jest w ramach wyodrębnionych obszarów działania. Obszary działania przyporządkowane są poszczególnym członkom Zarządu. Członek Zarządu sprawuje bezpośredni nadzór nad przyporządkowanym mu obszarem działania. Wyodrębnienia obszarów działania dokonuje Zarząd, zaś przyporządkowania obszarów działania poszczególnym członkom Zarządu dokonuje prezes Zarządu.

W ramach obszarów działania funkcjonują piony, grupujące jednostki organizacyjne (departamenty, biura, linie biznesowe, regionalne centra sprzedaży) wyodrębnione w KIR i przyporządkowane do danego pionu. Bezpośredni nadzór nad danym pionem sprawuje dyrektor zarządzający.

Organem opiniodawczo – doradczym KIR jest Kierownictwo, które stanowią członkowie Zarządu, dyrektorzy zarządzający oraz dyrektor Departamentu Prawnego.

W KIR powołany został, z uwzględnieniem wymogów wynikających z Wymagań nadzorczych w zakresie odporności cybernetycznej dla infrastruktur rynku finansowego (Cyber resilience oversight expectations for financial market infrastructures), Komitet ds. Bezpieczeństwa i Ryzyka.

Komitet ds. Bezpieczeństwa i Ryzyka, pod przewodnictwem Przewodniczącego – członka Zarządu, zapewnia nadzór nad:

1) skuteczną i terminową realizacją działań korygujących oraz obserwacji i zaleceń audytorów wewnętrznych i zewnętrznych;
2) wszystkimi aspektami ryzyka oraz

3) wdrożeniem Strategii cyberodporności w KIR, Ram cyberodporności w KIR oraz zasad, procedur i środków kontrolnych w tym zakresie.

Komitet ds. Bezpieczeństwa i Ryzyka pełni także funkcje kontrolne w zakresie:

1) skuteczności wdrożonych mechanizmów bezpieczeństwa;
2) realizacji działań strategicznych i operacyjnych w zakresie bezpieczeństwa;
3) realizacji planów postępowania z ryzykiem oraz procesu przygotowania i utrzymania adekwatności Planu naprawy KIR i Planu uporządkowanej likwidacji KIR.

W zakresie swojego działania Komitet ds. Bezpieczeństwa i Ryzyka koncentruje się na zagadnieniach bezpieczeństwa i cyberbezpieczeństwa.

Zarządzanie ryzykiem w KIR realizowane jest na podstawie dokumentacji przyjętej w ramach Systemu Zarządzania Ryzykiem (SZR). Głównym celem SZR jest zapewnienie takich warunków działania KIR, żeby minimalizować prawdopodobieństwo wystąpienia strat. System stworzono w celu rozpoznawania rodzaju ryzyka, z jakim KIR może mieć do czynienia, jego pomiaru i kontrolowania.

Na dokumentację SZR składają się:

1) Strategia zarządzania ryzykiem w KIR;
2) Zasady zarządzania ogólnym ryzykiem prowadzenia działalności w KIR;
3) Zasady analizy krytyczności procesów oraz zarządzania ryzykiem operacyjnym i ryzykiem naruszenia bezpieczeństwa w KIR;
4) Zasady zarządzania ryzykiem kredytowym i płynności w KIR;
5) Zasady zarządzania ryzykiem powierniczym i inwestycyjnym w KIR;
6) Procedura identyfikowania scenariuszy w KIR;
7) Plan naprawy Krajowej Izby Rozliczeniowej S.A.;
8) Plan uporządkowanej likwidacji Krajowej Izby Rozliczeniowej S.A.;
9) Plan podwyższenia kapitału własnego Krajowej Izby Rozliczeniowej S.A.;
10) Polityka informacyjna Krajowej Izby Rozliczeniowej S.A.;
11) Zasady ujawniania informacji w KIR zakresie dotyczącym systemów płatności.

Dodatkowo w KIR wdrożono Strategię cyberodporności w KIR oraz Ramy cyberodporności w KIR.

W zakresie systemów płatności zarządzanie zorganizowano w dwóch liniach biznesowych – Linii biznesowej rozliczenia sesyjne oraz Linii biznesowej płatności natychmiastowe.

W KIR funkcjonuje System kontroli wewnętrznej, którego celem jest wspomaganie zarządzania KIR, przyczyniając się do zapewnienia w szczególności:

1) efektywności i wydajności wykonywanych przez KIR zadań;
2) zgodności działania z powszechnie obowiązującymi przepisami prawa i regulacjami wewnętrznymi oraz Strategią KIR;
3) identyfikacji i adekwatności ponoszonego ryzyka;
4) wiarygodności sprawozdawczości finansowej.

Elementem Systemu kontroli wewnętrznej jest Departamentu Audytu Wewnętrznego, który podlega bezpośrednio prezesowi Zarządu. Zadaniem Departamentu Audytu Wewnętrznego jest dostarczenie Zarządowi niezależnych i obiektywnych informacji oraz ocen we wszystkich audytowanych obszarach z uwzględnieniem prawidłowości systemu kontroli wewnętrznej. Wdrożone w KIR regulacje o charakterze operacyjnym określają możliwe do podjęcia działania w przypadku wystąpienia zdarzeń mogących potencjalnie zagrażać KIR w prowadzeniu kluczowej działalności oraz świadczeniu kluczowych usług. Są to:

1) Plan Ciągłości Działania (który jest elementem procesu zarządzania ciągłością działania KIR, określonego w Zasadach zarządzania ciągłością działania KIR, obejmujących w szczególności Strategię zachowania ciągłości działania KIR);
2) Plan naprawy Krajowej Izby Rozliczeniowej S.A.;
3) Plan uporządkowanej likwidacji Krajowej Izby Rozliczeniowej S.A.;
4) Plan podwyższenia kapitału własnego Krajowej Izby Rozliczeniowej S.A..

KIR przeprowadza testy warunków skrajnych, korzystając z opracowanych scenariuszy (w zakresie wystąpienia zdarzeń mogących potencjalnie zagrażać KIR w prowadzeniu kluczowej działalności oraz świadczeniu kluczowych usług) w celu:

1) określenia możliwych do podjęcia działań przez KIR w ramach Planu naprawy Krajowej Izby Rozliczeniowej S.A. lub Planu uporządkowanej likwidacji Krajowej Izby Rozliczeniowej S.A.;
2) identyfikacji dodatkowych źródeł ogólnego ryzyka prowadzenia działalności, a także oceny ich potencjalnego wpływu na działalność i usługi świadczone przez KIR;
3) oszacowania kwoty płynnych aktywów netto finansowanych kapitałem, wynikającej z profilu ogólnego ryzyka prowadzenia działalności KIR, pozwalającej na wdrożenie działań przewidzianych w ramach Planu naprawy Krajowej Izby Rozliczeniowej S.A. lub Planu uporządkowanej likwidacji Krajowej Izby Rozliczeniowej S.A..

Podstawowymi mechanizmami kontrolnymi są testy w warunkach skrajnych na bazie przyjętych scenariuszy i opcji naprawczych.

Proces identyfikacji, analizy i oceny ryzyka prowadzony jest zgodnie z przyjętymi w KIR regulacjami wewnętrznymi. Proces analizy ryzyka odbywa się cyklicznie oraz doraźnie, w przypadku wystąpienia zdarzenia powodującego potrzebę przeprowadzenia takiej analizy poza wyznaczonym do tego czasem. W ramach procesu analizowane są ryzyka: kredytowe, płynności, prawno-regulacyjne, prowadzenia działalności, operacyjne (i naruszenia bezpieczeństwa), ryzyko powiernicze oraz ryzyko inwestycyjne.

Proces identyfikacji, analizy i oceny ryzyka prowadzony jest zgodnie z najlepszymi praktykami rynkowymi i normami międzynarodowymi (ISO 22301 oraz ISO 27001).

W KIR wdrożono sformalizowane i certyfikowane na zgodność z normą ISO 22301 mechanizmy identyfikacji krytycznych funkcji (System zarządzania ciągłością działania). Cyklicznie przeprowadzana jest analiza krytyczności procesów, której elementem jest analiza ryzyk strategicznych i operacyjnych, analiza z obszaru ochrony danych, analiza ryzyka dla zasobów (wyznaczanie poziomu strat finansowych i pozafinansowych), a także wskazanie podatności i prawdopodobieństwa niedostępności i ryzyka utraty dostępności.

W ramach prowadzonej analizy ryzyka realizowanej dwa razy w roku identyfikowane są wszelkie zasoby niezbędne dla realizacji procesów KIR, zagrożenia i wymagane zabezpieczenia minimalizujące możliwość materializacji ryzyka. Dla zidentyfikowanych funkcji/procesów krytycznych określane są zabezpieczenia dokumentowane w Planie Ciągłości Działania.

W KIR wdrożono proces zarówno testowania - potwierdzenia adekwatności oraz skuteczności zaplanowanych mechanizmów zabezpieczających, jak i odpowiedzialność za przegląd systemu (dokumentacji), adekwatność wymogów oraz aktualność wszelkich elementów operacyjnych. System zarządzania ciągłością działania jest kluczowym elementem oceny ryzyka i adresuje kwestie takie jak identyfikacja innych/powiązanych procesów, a także jest częścią procesu podejmowania istotnych decyzji wewnętrznych, w tym mechanizmów zarządzania zmianą w obszarze IT.

Wyniki wszystkich aspektów oceny ryzyka w KIR nadzorowane są przez powołany specjalnie w tym celu Komitet ds. Bezpieczeństwa i Ryzyka, jak również przez Zarząd. KIR regularnie dokonuje przeglądów i audytów swoich systemów, polityki, procedur i mechanizmów kontroli. Wszystkie elementy wprowadzonego SZR podlegają cyklicznym audytom wewnętrznym oraz zewnętrznym (kontrolnym i certyfikacyjnym), przeprowadzanym przez akredytowanych audytorów sprawdzających zgodność ww. systemów z wymaganiami norm ISO 27001 oraz ISO 22301. Wyniki audytów są komunikowane interesariuszom.