Appendix No. 2 to Resolution of the Management Board No. 33/2023 dated 27 February 2023

Disclosure report on management principles

Krajowa Izba Rozliczeniowa S.A.

Description of management principles at Krajowa Izba Rozliczeniowa S.A.
– information for the participants in payment systems

As of 1 February 2023

Krajowa Izba Rozliczeniowa S.A. (KIR) is a joint-stock company with the following shareholders: 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. and Związek Banków Polskich (Polish Bank Association).

Participation of individual shareholders in the share capital of KIR is presented, also graphically, at the following address: https://www.kir.pl/o-nas/akcjonariat/.

KIR's governing bodies are: General Meeting of Shareholders, Supervisory Board and Management Board.

According to the Articles of Association of Krajowa Izba Rozliczeniowa S.A., the Supervisory Board is comprised of at least 9 members appointed separately by each of the shareholders having at least 300 shares. The National Bank of Poland has the right to appoint one member of the Supervisory Board, regardless of its participation in the KIR's shareholding structure. The member of the Supervisory Board appointed by a shareholder may be dismissed only by the same shareholder, and the shareholder may appoint another person in their stead. The shareholder may only appoint a member of its management board or its employee having the right education and experience in the financial sector to be a member of the Supervisory Board.

The Supervisory Board holds constant supervision over the operations of KIR.

Currently, the Supervisory Board of the 11th term is comprised of 12 members. The Chairperson of the Supervisory Board is a member of the Supervisory Board appointed by the National Bank of Poland.

As part of its competences, the Supervisory Board established two standing committees, that is the Remuneration Committee and the Audit and Risk Committee. Pursuant to the regulations of these committees, they are comprised of at least three members appointed with a resolution of the Supervisory Board from among its members. The Remuneration Committee and the Audit and Risk Committee currently are comprised of 5 members each.

The Remuneration Committee is to support the Supervisory Board with regard to the policy on remuneration of members of the Management Board and other terms and conditions of employment of the members of the Management Board, and to offer support within the scope of appointing and dismissing members of the Management Board.

The Audit and Risk Committee is to advise the Supervisory Board on the issues of supervision over the proper application of financial reporting rules at KIR, and to cooperate with expert auditors and advise the Supervisory Board within the scope of supervision over the operation of the risk management system at KIR.

Pursuant to the Articles of Association of Krajowa Izba Rozliczeniowa S.A., the Management Board is comprised of 3 to 6 members appointed by the Supervisory Board for a three-year joint term. The works of the Management Board are headed by the president of the Management Board.

The Management Board manages the ongoing operations of KIR and makes decisions on all matters not reserved to the Supervisory Board and the General Meeting of Shareholders.

The Management Board fulfils its information obligations towards the Supervisory Board in accordance with the Act of 15 September 2000 on the Code of Commercial Companies and Partnerships.

At present, the Management Board is comprised of three experienced managers who, in their professional careers, held major managerial positions in prestigious financial market entities. The professional profile of the members of the Management Board is linked with financial institutions where their managerial functions were each time associated with IT technology.

KIR conducts its activities in separate areas of operation. Individual areas of operation are assigned to individual members of the Management Board. A member of the Management Board directly supervises their assigned area of operation. The areas of operation are established by the Management Board, and then assigned to individual members of the Management Board by the President of the Management Board.

Within individual areas of operation, there are divisions which group the organisational units (departments, offices, business lines, regional sales centres) created in KIR and assigned to a given division. A given division is directly supervised by the managing director.

The opinion- and advice-giving body of KIR is the Management that is comprised of the members of the Management Board, managing directors and head of the Legal Department.

The Security and Risk Committee was established in KIR with consideration given to cyber resilience oversight expectations for financial market infrastructures.

Headed by the Chairperson, a member of the Management Board, the Security and Risk Committee holds supervision over:

1) effective and on-time performance of corrective measures, and observations and recommendations of internal and external auditors;
2) all aspects of risk, and
3) implementation of the Cyber-resilience Strategy at KIR, Cyber-resilience Frameworks at KIR, as well as principles, procedures and control measures in that respect.

The Security and Risk Committee also performs control functions within the scope of:

1) effectiveness of the implemented security mechanisms;
2) performance of strategic and operational measures within the scope of security;
3) execution of plans for handling risk, and the process of preparation and maintenance of adequacy of the KIR's Recovery Plan and KIR's Orderly Wind-down Plan.

Within the scope of its operations, the Security and Risk Committee focuses on the issues of security and cyber-security.

Risk is managed in KIR on the basis of documentation adopted as part of the Risk Management System (RMS). The main goal of RMS is to ensure the conditions for the operation of KIR that allow it to minimise the probability of losses. The system is designed in order to identify, measure and control the risk that KIR may face.

The RMS documentation is comprised of:

1) Risk management strategy at KIR;
2) Principles of general business risk management at KIR;
3) Principles of process criticality analysis, and operational risk and security breach risk management at KIR;
4) Principles of credit and liquidity risk management at KIR;
5) Principles of custody and investment risk management at KIR;
6) Scenario identification procedure at KIR;
7) Recovery Plan of Krajowa Izba Rozliczeniowa S.A.;
8) Orderly Wind-down Plan of Krajowa Izba Rozliczeniowa S.A.;
9) Equity Increase Plan of Krajowa Izba Rozliczeniowa S.A.;
10) Information Policy of Krajowa Izba Rozliczeniowa S.A.;
11) Principles of information disclosure at KIR with regard to payment systems.

Additionally, KIR implemented the Cyber-resilience Strategy at KIR and the Cyber-resilience Frameworks at KIR.

Within the scope of payment systems, the management is organised into two business lines: Session clearing business line and Instant payment business line.

KIR has the Internal control system aimed at supporting the management of KIR and helping particularly to assure:

1) effectiveness and efficiency of tasks performed by KIR;
2) compliance of operations with the commonly applicable provisions of the law, internal regulations and KIR Strategy;
3) identification and adequacy of the incurred risk;
4) credibility of financial reporting.

The Internal Audit Department is an element of the Internal Control System that is subordinate directly to the President of the Management Board. The Internal Audit Department is to provide the Management Board with independent and objective information and assessments in all audited areas, with consideration given to the correctness of the internal control system. The operational regulations implemented in KIR define possible actions in the case of occurrence of events that might potentially threaten KIR while performing its key operations and providing key services. They are:

1) Operation Continuity Plan (which is an element of the operation continuity management process in KIR set forth in the KIR's Principles of operation continuity management covering, in particular, the KIR's Strategy for operation continuity maintenance);
2) Recovery Plan of Krajowa Izba Rozliczeniowa S.A.;
3) Orderly Wind-down Plan of Krajowa Izba Rozliczeniowa S.A.;
4) Equity Increase Plan of Krajowa Izba Rozliczeniowa S.A.

KIR conducts tests of extreme conditions with the use of developed scenarios (within the scope of occurrence of events that may potentially threaten KIR while performing its key operations and providing key services) in order to:

1) define possible actions that may be taken by KIR as part of the Recovery Plan of Krajowa Izba Rozliczeniowa S.A. or the Orderly Wind-down Plan of Krajowa Izba Rozliczeniowa S.A.;
2) identify additional sources of general business risk, and assessment of their potential impact on the operations and services provided by KIR;
3) estimate the amount of liquid net assets funded by equity arising from the profile of general business risk of KIR that allows for the implementation of actions provided for in the Recovery Plan of Krajowa Izba Rozliczeniowa S.A. or Orderly Wind-down Plan of Krajowa Izba Rozliczeniowa S.A.

The basic control mechanisms are tests in extreme conditions on the basis of adopted scenarios and corrective options.

The process of risk identification, analysis and assessment follows the internal regulations adopted at KIR. The process of risk analysis takes place periodically and on an ad-hoc basis if an event occurs which necessitates the performance of such analysis outside the predefined date. In this process the following types of risks are analysed: credit, liquidity, legal and regulatory, business, operational (and security breach), custody and investment risk.

The process of risk identification, analysis and assessment follows the best market practices and international standards (ISO 22301 and ISO 27001).

KIR implemented formalised and ISO-22301-certified mechanisms for critical function identification (Operation continuity management system). The process criticality analysis is conducted periodically and involves the strategic and operational risk analysis, personal data protection analysis, analysis of risk for resources (setting the level of financial and non-financial losses), as well as indication of vulnerability and probability of unavailability and the risk of loss of availability.

As part of the risk analysis conducted twice a year, all resources necessary to complete the KIR processes, threats and safety measures required to minimise the possibility of risk materialisation are identified. Safety measures are specified for the identified critical functions/ processes and documented in the Operation Continuity Plan.

KIR implemented both the process of testing to confirm the adequacy and efficiency of the planned security mechanisms and the responsibility for the review of the system (documentation), adequacy of requirements and topicality of all operational elements. The operation continuity management system is a key element of the risk assessment and deals with such issues as the identification of other/related processes, while being a part of the process of making important internal decisions, including change management mechanisms in the IT area.

The results of all aspects of risk assessment at KIR are supervised by the specially appointed Security and Risk Committee and the Management Board. KIR regularly conducts reviews and audits of its systems, policies, procedures and control mechanisms. All elements of the introduced RMS are subject to periodical internal and external audits (control and certification audits) conducted by accredited auditors who verify the compliance of the above-mentioned systems with the requirements of the ISO 27001 and ISO 22301 standards. The audit results are communicated to the stakeholders.