

APPROVED  
by the Board of Directors of JSC RusHydro  
(Minutes dated 4 April 2008 No. 50)

**Regulations on the JSC RusHydro Compliance  
and Risk Management Policy**

# CONTENTS

- 1. GENERAL PROVISIONS, KEY TERMS AND DEFINITIONS**
  - 1.1. General provisions
  - 1.2. Key terms and definitions
- 2. OBJECTIVES AND PURPOSE OF THE POLICY, KEY GOALS AND TASKS OF THE COMPLIANCE AND RISK MANAGEMENT SYSTEM**
  - 2.1. Objectives and purpose of the policy
  - 2.2. Key goals and tasks of the Compliance and Risk Management System
- 3. POLICY PRINCIPLES**
- 4. METHODS OF AND APPROACHES TO RISK MANAGEMENT AND COMPLIANCE CONTROL**
  - 4.1. Chief compliance control methods and procedures
    - 4.1.1. Chief compliance control methods
    - 4.1.2. Chief compliance control procedures
  - 4.2. Chief compliance control processes
    - 4.2.1. Business process analysis
    - 4.2.2. Assessment of existing control procedures
    - 4.2.3. Development of control procedures
    - 4.2.4. Monitoring
  - 4.3. Chief risk management processes and methods
    - 4.3.1. Risk identification
    - 4.3.2. Risk classification
    - 4.3.3. Determination of the risk tolerance level
    - 4.3.4. Risk assessment and analysis
    - 4.3.5. Risk management methods
    - 4.3.6. Development of risk management measures
    - 4.3.7. Risk management monitoring
    - 4.3.8. Training
  - 4.4. Chief processes in the internal audit sphere
    - 4.4.1. Periodical assessment of the effectiveness of the Compliance and Risk Management System
    - 4.4.2. Sample testing of material facts
- 5. REQUIREMENTS OF AND RESTRICTIONS ON COMPLIANCE CONTROL AND RISK MANAGEMENT**
- 6. IMPLEMENTATION OF THE COMPLIANCE AND RISK MANAGEMENT POLICY**
  - 6.1. General structure of the Compliance and Risk Management System
    - 6.1.1. Compliance System (CS)
    - 6.1.2. Risk Management System (RMS)
  - 6.2. Functional structure and distribution of powers
    - 6.2.1. Board of Directors of the Company
    - 6.2.2. Auditing Committee under the Board of Directors of the Company
    - 6.2.3. Management Board of the Company
    - 6.2.4. Authorised Risk Management Body under the Chairman of the Management Board
    - 6.2.5. Member of the Management Board responsible for compliance and risk management
    - 6.2.6. Structural subdivisions of the Company responsible for risk management and compliance
    - 6.2.7. Heads of structural subdivisions and branches of the Company
    - 6.2.8. Company staff
  - 6.3. Regulatory documents in the sphere of compliance and risk management

## **1. GENERAL PROVISIONS, KEY TERMS AND DEFINITIONS**

### **1.1. General provisions**

These Regulations establish the main principles for the organisation and functioning of the Compliance and Risk Management System of JSC RusHydro (hereinafter referred to as the Company).

The Company's policy in the sphere of compliance and risk management is based on the recommendations of the best world practices and meets all the requirements of the Russian legislation.

The Company's Compliance and Risk Management System constitutes the aggregate of the organisational structure, methodologies and procedures adopted by the management of the Company as means for the Company to structure and conduct its financial and business activities efficiently.

**Compliance** is a process designed to provide reasonable guarantees of achieving the goals of efficient and productive use of the Company's resources, safekeeping of assets, observance of legislative requirements and presentation of accurate financial statements.

**Risk management** is a cyclical process including identification of critical situations that might impact on the Company achieving its objectives and disrupt its operational and investment activities; their assessment; development and implementation of measures to reduce their probability and damage caused; control over the effectiveness of these measures.

The Company's Compliance and Risk Management System is orientated primarily on achieving an optimal balance between growth of the Company's value, its profitability and risks.

The Company's Compliance and Risk Management System helps keep assets safe, reduce risks, make the Company more manageable, form accurate reporting and fulfil the effective rules of the legislation and provides the Company's management with a reasonable guarantee of achieving the strategic and operating goals.

These Regulations are binding on all structural subdivisions and branches of the Company, subsidiaries and dependent companies (hereinafter referred to as SDC).

Amendments and addenda to these Regulations shall be introduced as required in the event of transformation of the benchmarks, organisational and functional structure and/or operating conditions of the Company.

Proposals to amend this Policy may be entered by a Member of the Management Board of the Company, the Chairman of the Management Board of the Company, the Management Board or the Board of Directors of the Company. Responsibility for organising reviews of proposals and initiating introduction of amendments shall be borne by the Chairman of the Management Board of the Company.

Amendments are subject to consideration and approval in accordance with the procedure determined by local by-laws of the Company.

## 1.2. Key terms and definitions

**Risk owner** is the Company employee that, by virtue of his/her powers and official duties, may and should manage this risk.

**Risk identification** is a continuous process of revealing, describing and documenting risks capable of impacting on the Company's business and formation of a register of the Company's risks.

**Risk chart** is a graph depicting Company risks identified and containing an assessment of the likelihood of risks being realised and of the possible damage, demonstrating the location of risk assessments in relation to one another.

**Capital at risk** is the damage caused by risk realisation multiplied by the likelihood thereof.

**Critical risk** is risk the damage from which is above the Company's level of tolerance and that is subject to priority management.

**Risk management measure** is a planned action designed to reduce the damage from and/or probability of risks.

**Risk management monitoring** means control over changes in risks and effectiveness of realisation of risk management measures.

**Risk assessment** is the process of determining the characteristics of the Company's risks. Use of mathematical calculation methods presupposes a *quantitative* assessment of the Company's risks, while use of expert methods implies a *qualitative* assessment.

**Risk prioritisation** is a qualitative assessment of the Company's risks for the purpose of identifying critical risks facing the Company and subsequently managing them.

**Risk register** is an organised list of the Company's risks containing information about the risks identified, the source of the information, the risk management measures undertaken and the risk owner.

**Risk** is a random event with two characteristics: (1) likelihood of the event's onset (beginning of its onset); (2) damage as a consequence of the onset of this event.

**Compliance and Risk Management System** is the aggregate of elements including the organisational structure, procedures, functions, responsibility of and staff involved in the Company's compliance control and risk management.

**Structural unit** is a structural subdivision or branch of the Company or an SDC.

**Structural subdivision** is a subdivision of the approved organisational structure of the Company's Executive Apparatus.

**Risk Management Department** is the structural subdivision whose terms of reference include the functions of managing risks within the Company.

**Compliance Department** is the structural subdivision whose terms of reference include the function of implementing compliance within the Company.

**Value at risk** is the mathematical expectation of discounted cash flows of the Company adjusted for risk.

**Risk tolerance** means the maximum losses not exerting a material impact on the Company's business and/or its KPI.

**Authorised Risk Management Body under the Chairman of the Management Board** is the management committee or other management body of the Company assigned, by resolution of the Chairman of the Company's Management Board, risk management functions and powers.

**Branch** is a separate subdivision of the Company located away from the Company and fulfilling all or some of the Company's functions, including representation functions.

**Member of the Management Board responsible for compliance and risk management** means the Member of the Company's Management Board assigned, in accordance with an Order on distribution of powers, the functions of organising compliance and of risk management.

## **2. OBJECTIVES AND PURPOSE OF THE POLICY, KEY GOALS AND TASKS OF THE COMPLIANCE AND RISK MANAGEMENT SYSTEM**

### **2.1. Objectives and purpose of the policy**

The main objective of the Policy in the sphere of compliance and risk management is to determine the binding principles of the Company's Compliance and Risk Management System and to form a unified approach to fulfilling the processes of compliance and of risk management within the Company.

These Regulations are intended for providing information about the key principles of the compliance and risk management system of the Company to interested parties: shareholders, auditors, portfolio and strategic investors, financial and investment analysts, and others.

### **2.2. Key goals and tasks of the Compliance and Risk Management System**

The key goals of the Company's Compliance and Risk Management System are:

- to provide for implementation of the Company's strategy;
- to preserve and make efficient use of the Company's resources and potential;
- to adapt the Company promptly to changes in the internal and external environment;
- to provide for efficient functioning of the Company, its stability and development prospects.

For the purpose of achieving these goals, the Company's Compliance and Risk Management System tackles the following crucial tasks:

- to reduce the number of unforeseen circumstances and minimise losses in business activities through efficient fulfilment of the following functions:
  - identification of all risks jeopardising the stability of production activities, financial stability and attainment of the Company's strategic goals;
  - analysis of the risks identified for the purpose of making the most accurate assessment of the damage and the likelihood of their realisation;

- quality information and analytical support for financial, investment, and asset portfolio structuring decision-making;
- prompt resolution of conflicts of interest arising in the Company’s activities;
- justified decision-making on insurance of the Company’s risks;
- creation of reserves ensuring continuity of the Company’s activities;
- to ensure control over:
  - correct implementation of decisions taken by the Company’s management bodies;
  - creation of the requisite internal regulatory documents;
  - fulfilment of the requirements of external and internal regulatory documentation applicable to the Company’s activities;
  - safe-keeping of the Company’s assets;
  - formation of full and accurate information about the activities of the Company and its property status required by internal and external users of the financial statements;
  - distribution of powers and functions among the structural units of the Company, preclusion of duplication and completeness of distribution;
- to provide the Company’s management with the requisite information about divergences from the rules adopted for the functioning of the Compliance and Risk Management System;
- to ensure timely preparation of full and accurate reporting with respect to disclosure of risk information;
- to exercise control over the procedures for disclosing material information about the Company’s activities to external users according to the following criteria:
  - accuracy of the information disclosed at all stages of its collection and processing;
  - observance of the regulations governing information disclosure.

### **3. POLICY PRINCIPLES**

The Company’s policy in the sphere of compliance and risk management is based on the following key principles:

- **continuity:** the Company’s Compliance and Risk Management System functions continuously;
- **integrity:** the Compliance and Risk Management System is an integral part of corporate governance system within the Company;
- **comprehensiveness:** the Compliance and Risk Management System embraces all the Company’s spheres of activity and all the types of risk arising within their framework. Control procedures exist in all the Company’s business processes at all levels of management;

- **methodological unity:** processes are implemented under the Compliance and Risk Management System on the basis of unified approaches and standards for all the Company's structural units;
- **priority:** the Company undertakes the requisite measures primarily in relation to risks that are critical for the Company's business;
- **information disclosure:** the Compliance and Risk Management System ensures that control is exercised over procedures for disclosing information about the Company's activities to external users;
- **functionality:** responsibility for management of risks in the Company's various spheres of activity is distributed in accordance with the division of functional duties within the Company;
- **division of duties:** functions are distributed among staff and structural units of the Company in such a way that no employee or structural subdivision is concurrently fulfilling functions and exercising control over their fulfilment;<sup>[1]</sup>
- **optimality:** the volume and complexity of the compliance procedures and risk management measures undertaken within the Company are necessary and sufficient for fulfilment of the tasks and achievement of the objectives of the Compliance and Risk Management System;
- **equilibrium:** means and powers are provided to each structural unit or member of staff of the Company for fulfilling all controlling functions and risk management functions;
- **precise regulation:** all operations are performed in compliance with the procedure stipulated by the by-laws of the Company;
- **timely notification:** information about risks identified and failure to fulfil controlling functions shall be provided in a timely manner to the persons authorised to pass relevant decisions;
- **permission and approval:** within the Company, all financial and business operations shall be officially approved or permitted by responsible persons within the bounds of their terms of reference;
- **adaptability:** the Company's Compliance and Risk Management System shall be regularly updated for the purpose of identifying all potential business risks and ensuring maximally efficient application of control and risk management methods.

#### **4. METHODS OF AND APPROACHES TO RISK MANAGEMENT AND COMPLIANCE CONTROL**

##### **4.1. Chief compliance control methods and procedures**

The following complex of compliance control methods and procedures established by the management in individual business spheres and sectors shall be applied within the Company for the purpose of ensuring efficient and reliable Company governance:

#### 4.1.1. Chief compliance control methods

**Appropriate division of responsibility** within the Company is achieved by distributing duties between employees at the level of job descriptions and interaction regulations and by exercising dual control over the performance of material business operations. For the purpose of reducing the risk of human error or fraud, one and the same person is not permitted in the Company to combine the functions of sanctioning, fulfilling and controlling performance of business operations. The principles of division of powers and responsibility among structural units at each level of management (vertically) and within each level of management (horizontally) are regulated by by-laws of the Company, document flow charts and regulations on interaction between structural units.

**The authority confirmation system** adopted within the Company makes it possible to determine precisely the bounds within which employees operate in fulfilling their duties and includes in-house documents:

- regulating the decision-making procedure for specific spheres of activity, determining the persons responsible for decision-making and indicating the bounds of their authority;
- determining who has the right to sign source documents (where the position, full name and level of competence, i.e., type or kinds of operation on which the official is entitled to make decisions, are to be indicated);
- describing the course followed by documents for agreement (signing), sanctioning, imposition of resolutions and approval of documents by the management for decision-making purposes;
- establishing the system of passwords allowing responsible persons to gain access to assets, documents and information contained in information systems.

**Documenting and systemic recording** in information systems are the basic forms of documentary control within the Company. All economic operations are formalised by source documents that are booked on the condition that they are drawn up in unified source document formats or formats developed by the Company and contained in its by-laws.

**The physical methods** applied within the Company **for controlling and protecting** assets, documents and data in information systems are designed to restrict unsanctioned access to the Company's property. Company in-house documents determine the people responsible for the safe-keeping and movement of assets and written agreements on material liability are concluded with them in the manner established by the legislation. For the purpose of ensuring protection of tangible assets against physical harm (accidental destruction, spoilage as a result of failure to observe storage conditions and regimes), duly equipped storage facilities are set up within the Company. Information about the Company's business operations is stored in hard copy and (or) electronically. Documents are stored in compliance with the Company by-laws. The right to direct access to information about the Company's business activities is enjoyed by:

- Company employees whose duties include compiling, processing, disseminating, accumulating, storing, using and transmitting such information to interested parties;
- Company officials whose duties include using such information, as well as agreeing, certifying and approving documents containing this information.

The other Company employees have special access to information restricted by position-determined access rights; access rights according to the route taken by the information; access rights granted by written permission of the authorised Company official. The list of officials entitled to give permission to access specific information about economic activities is established by the by-laws

and directive documents of the Company. Classification of information on the Company's business activities as confidential and the liability of Company employees for disclosing it are established by the legislation of the Russian Federation and the Company in-house documents (orders, directives, etc.). In accordance with the requirements of the legislation, the Company performs inventories of assets and liabilities, the procedure for these being set out in the Company by-laws.

**Independent audits** are performed by staff of the Compliance Department and the Internal Audit Commission on the basis of developed and approved audit plans.

#### **4.1.2. Chief compliance control procedures**

**Document agreement** is a procedure by which the controlling authority checks and confirms, within the bounds of its terms of reference, the accuracy, completeness and consistency of the information contained in a document, its correct execution and compliance with the by-laws, as well as the existence of the requisite appendices and accompanying documents.

**Document approval** is a procedure by which the authorised person or body puts a document into effect.

**Data reconciliation** is a check carried out of the integrity and consistency of information received from different sources, making it possible to identify potential information entry and processing errors in the early stages, before the reporting documents are drawn up.

**Key performance indicator monitoring** means analysis of compliance between actual budget indicators and the planned ones, the purpose being to identify trends not characteristic of the Company's activities. Substantial divergences constitute grounds for initiating an additional check to disclose errors or for analysing the need to find the reasons for the divergences.

**Supervision over observance of information disclosure regulations** means revealing of divergences in routes and time schedules of reporting documents for the purpose of taking relevant corrective steps to bring information disclosure into line with the established procedure. This is carried out by authorised controlling bodies and officials of the Company.

**Division of access rights** is use of software and hardware to exercise control over information provided to Company employees in the context of division of duties.

**Automated information entry and transformation** presupposes templates and filters for entering data into electronic reporting forms, automatic calculation procedures installed in data processing programmes and reporting form creation procedures.

#### **4.2. Chief compliance control processes**

##### **4.2.1. Business process analysis**

Analysis of the Company's business processes is carried out under the management of the Compliance Department for the purpose of determining the key control points and means of control and assessing their appropriateness.

Business processes are analysed according to the principle of process chains reflecting the successive fulfilment of functions, links between events and functions within the scope of the business process.

#### **4.2.2. Assessment of existing control procedures**

As a result of business process analysis, the Compliance Department assesses existing control procedures and identifies those that are lacking and thus entailing risk events.

The effectiveness of control procedures is assessed with respect to ensuring a reasonable guarantee of achieving the relevant goals of the business process under study.

A list is drawn up of lacking control procedures, as well as ones requiring updating or processing, for the purpose of excluding, in the future, the possible occurrence of risk events that might result in extraordinary (unregulated) situations.

#### **4.2.3. Development of control procedures**

Control procedures are elaborated under the guidance of the Compliance Department by means of forming a complex of measures designed to reduce the likelihood of risks occurring and mitigate their adverse impact.

Specific measures (financial, marketing, legal and organisational) for minimising or eliminating risks are developed on the basis of the standard control procedures within the Company and in consideration of the reasons for and consequences of a given risk.

#### **4.2.4. Monitoring**

Monitoring of the compliance system consists in a mechanism for systematic supervision over the state of the Company's control procedures, changes in them, their application and effectiveness, for the purpose of prompt identification of negative trends, analysis of the results of the observations and preparation of data for management decision-making in the compliance sphere. Monitoring is carried out by the Compliance Department.

Monitoring includes the following procedures:

- determination of the person within the structural unit responsible for performance of a control procedure;
- analysis of control procedure implementation, identification of implementation problems and divergences, including in the auditing of Company structural units;
- preparation of periodical reports on control procedure performance.

The main method used in monitoring fulfilment of control procedures is time monitoring, i.e., determination of control points in development, agreement, approval and introduction.

### **4.3. Chief risk management processes and methods**

#### **4.3.1. Risk identification**

Identification of risks envisages disclosure, description and documentation of risks capable of affecting the Company's business and compilation of a register of the Company's risks. The risk register should be regularly updated. Risks are identified by the staff of Company structural units. Collection, processing, analysis and systematization of information obtained on identified risks, as well as compilation of the risk register, are the responsibility of the Risk Management Department.

*Information collection* is carried out for the purpose of obtaining comprehensive information about risks, the nature of their emergence and current status by the following methods:

- analysis of available data on risks previously realised;
- questionnaires;
- interviews;
- analysis of in-house documents;
- analysis of external data;
- on-site engineering inspections.

Risk identification results in a risk register bringing together all information received about risks. The risk register has the following structure:

- source, that is, indication of the source of the information about the risk (report, interview, document, outside source);
- formulation of the risk containing a description of the possible event;
- risk category according to the developed classification system;
- current risk management measures, that is, measures taken currently to minimise the consequences of the risk;
- risk owner, that is, the Company employee that, by virtue of his/her powers and official duties, may and should manage this risk. Risk owners are determined for critical risks after their prioritisation;
- risk assessment is completed on the basis of the risk prioritisation results.

The prioritised Risk Register is approved by the Company's Management Board.

#### **4.3.2. Risk classification**

*Classification of the risks* in the register is carried out according to the following parameters:

1. In terms of materiality, risks are subdivided into:

- critical;
- non-critical,

according to the likelihood of their realisation and possible damage in relation to the tolerance level. The register identifies additional risk classification groups if required by the nature of the risks and the results of their assessment.

2. By the type of activity in which they occur, the Company's risks are subdivided into:

- operating risks – arising in the sphere of operation of hydro-engineering structures, sale of electric power and other current activities;

- investment activity risks – hampering timely implementation of investment projects of due quality and within the limits of the allocated financing.

3. By the nature of their emergence, risks are subdivided into:

- financial – associated with unfavourable market situations, inefficient management of finances, etc.;
- non-financial – political, social, reputational and environmental risks, risks of state regulation, project management, etc.

The number of risk classification groups by nature of emergence may be expanded if the character of the identified risks dictates the need for this.

The risk classification system is developed within the framework of the process of identifying and prioritising risks by the Risk Management Department and approved by the Chairman of the Management Board or the Authorised Risk Management Body under the Chairman of the Management Board.

#### **4.3.3. Determination of the risk tolerance level**

**Risk tolerance** means the maximum losses not exerting a material impact on the Company's business and/or its KPI.

*The risk tolerance level* is used in prioritising risks and identifying risks that are critical for the Company's activities. The process of determining tolerance includes consideration of a multitude of factors, among them indicators of the Company's financial status and the values of the level of risk perception by the management.

In view of the large volume of investment by the Company and the nature of the investment projects within the Company, two levels of tolerance are determined – *a level of tolerance to operating risks* (operation of power stations and sales) and *a level of tolerance to investment project risks*. This approach is necessary for correct assessment of operating and investment project risks.

For the purpose of determining risk tolerance, the Risk Management Department considers permissible divergences of the Company's key financial indicators and presents proposals for the Company's tolerance levels for consideration and approval by the Authorised Body under the Chairman of the Management Board.

#### **4.3.4. Risk assessment and analysis**

##### ***Risk prioritisation***

All the risks described in the register must be prioritised, meaning subjected to expert assessment for the purpose of determining which risks are critical for the Company. The risk prioritisation process is organised by the Risk Management Department and is performed by the Authorised Risk Management Body under the Chairman of the Management Board.

The risk prioritisation process includes the following steps:

- development and approval of an assessment scale;
- expert assessment of risks according to the scales developed;

- processing of data obtained from risk assessment and compilation of risk charts.

A risk assessment in accordance with the scales developed may be obtained by a variety of methods: questionnaires, interviews, ballots. The optimal method from the efficiency viewpoint is voting by the members of the Authorised Risk Assessment Body under the Chairman of the Management Board during their meeting.

### ***Processing and prioritisation results***

Processing of the results obtained includes:

- determination of aggregate assessments of harm and probability;
- structuring of risk charts;
- determination of the possible harm from risk realisation.

Risks causing harm above the adopted tolerance level are classed as critical.

Prioritisation of risks results in charts of the Company's risks, graphically demonstrating the results of the prioritisation, and a Risk Register identifying critical risks.

Risks recognised as critical on the basis of prioritisation results are subject to further analysis by the Authorised Risk Management Body under the Chairman of the Management Board and by the Management Board of the Company. Non-critical risks are managed within the scope of the official duties of each employee of the Company and the information on them is used in the subsequent management cycle of risk identification.

### ***Risk owners***

For risks assessed as critical during the prioritisation process, risk owners are assigned to be responsible for elaborating and implementing risk management measures. The Risk Management Department makes a proposal for deciding on the owners of critical risks proceeding from the essence of each individual risk, the factors giving rise to it, the nature of the potential damage and possible management measures. The list of critical risk owners is agreed with the critical risk owners and the Authorised Risk Management Body under the Chairman of the Management Board and is approved by the Management Board.

### ***Additional analysis***

Critical risks are subject to additional analysis for confirming (checking) the qualitative assessment of the probability and damage. Its scope might also include a quantitative assessment of the damage and probability for the purpose of making a more justified, economically effective decision on management of the risk. The main aim of the quantitative assessment is to determine as precisely as possible the amount of capital at risk, i.e., the possible damage from realisation of the risk multiplied by the probability of its realisation, as well as the value at risk, i.e., the mathematical expectation of discounted cash flows of the Company adjusted for the risk.

Critical risks are analysed by the owners of these risks with the methodological support of the Risk Management Department.

For the purpose of the additional analysis of critical risks, the *portfolio approach* is used. Interconnected critical risks, the emergence factors, characteristics and realisation effects of which are correlated, are analysed holistically for the purpose of assessing more precisely the probability

of their realisation and potential damage. It is the Risk Management Department that organises the interaction between risk owners required for holistic assessment of interconnected critical risks.

The risk charts and risk register are adjusted to comply with the results of the additional analysis.

#### **4.3.5. Risk management methods**

The Company uses the following risk management methods:

- risk taking;
- risk avoidance;
- risk transfer;
- risk control/mitigation.

##### ***Risk taking***

A risk is taken if all the methods available for mitigating it are economically unfeasible in comparison with the potential damage from realisation of the risk. The management is notified of the existence of this risk and its characteristics and they deliberately take no measures to impact on the risk.

##### ***Risk avoidance***

Risk avoidance involves terminating a specific type of activity (rejecting a project, withdrawing from a specific market). One way of avoiding risks is to change the strategic objective or operating process.

##### ***Risk transfer***

A decision to transfer a risk depends on the nature of the activity, the importance of the operation connected with the risk and its financial significance. Standard risk transfer mechanisms include: insurance, transfer of risks to partners within the scope of setting up a joint venture or association, outsourcing, diversification of the Company's activities and hedging.

##### ***Risk control/mitigation***

Risk control/mitigation is achieved by:

- organising a reporting system and formalising processes;
- conducting training programmes, involving Company staff in the Compliance and Risk Management System and developing the remuneration system;
- developing compliance and risk management methods and procedures;
- drawing up plans for ensuring business continuity, overcoming crises, preparing for natural disasters, ensuring safety at work and in hazardous situations;
- auditing (for instance, exercising control over performance indicators, drawing up incident reports, inspecting enterprises, comparing with international efficiency criteria, carrying out inspections).

The factors to be taken into consideration in selecting a risk management method are:

- compliance with corporate goals;
- costs/benefits of the decision made;
- availability of the requisite resources;
- compliance with regulatory documents.

#### **4.3.6. Development of risk management measures**

Development of action plans for managing critical risks is intended to reduce the damage and/or probability of risks. The measures must comply with the principle of economic feasibility – the cost of the measures introduced should not exceed the anticipated damage from realisation of the risk. Action plans are drawn up by risk owners and contain a precise determination of the tasks, who is responsible and the fulfilment time schedule.

The Risk Management Department consolidates the action plans drawn up for subsequent approval by the Management Board of the Company.

The portfolio approach is also used in developing critical risk management measures, taking into account the interconnection between the risks disclosed during the additional analysis. Consolidation of the action plans involves analysis of the impact of each of the proposed measures on the other risks. It is the Risk Management Department that organises the interaction between risk owners required for optimising action plans.

#### **4.3.7. Risk management monitoring**

*Risk management monitoring* presupposes control over changes in risks and effectiveness of risk management measures. Monitoring makes it possible to trace the status of the risk, determine whether the desired result of implementing one measure or another in the sphere of risk management has been achieved, whether sufficient information has been gathered for decision-making on risk management and whether this information has been used for reducing the degree of risk within the Company.

Monitoring is carried out by the Risk Management Department by collecting information about changes in critical risks and implementation of plans submitted by risk owners for introducing risk management measures. The Risk Management Department reports to the Management Board of the Company on the results of the monitoring.

Measures taken may be adjusted or new ones developed on the basis of the results of the monitoring.

#### **4.3.8. Training**

Company employees are trained on a regular basis for the purpose of transmitting knowledge and experience to new staff, monitoring trends in world risk management practice, updating the knowledge of employees and managers of all structural units in the risk management sphere.

#### **4.4. Chief processes in the internal audit sphere**

##### **4.4.1. Periodical assessment of the effectiveness of the Compliance and Risk Management System**

The effectiveness of the Compliance and Risk Management System is assessed periodically in order to determine the reliability of the compliance system and the likelihood of achieving the goals of the control procedures used by risk owners to manage the risks effectively. The periodical assessment is designed to prevent risks arising and is carried out in accordance with the audit plan approved by the Auditing Committee under the Board of Directors of the Company.

The process by which the effectiveness of the Compliance and Risk Management System is assessed includes the following stages:

- preliminary investigation of the compliance system applied to the Company's business processes;
- audit procedures including:
  - assessment of the design of control procedures;
  - assessment of control procedure implementation;
  - analysis of the components of the compliance system;
  - overall assessment of the effectiveness of the compliance system;
  - formulation of audit results;
- monitoring of fulfilment of recommendations based on the results of the audits.

##### **4.4.2. Sample testing of material facts**

Sample testing is performed on the initiative of the Board of Directors when a risk arises and is intended to investigate the reasons for its emergence connected with the inefficient functioning of the Compliance and Risk Management System.

#### **5. REQUIREMENTS OF AND RESTRICTIONS ON COMPLIANCE CONTROL AND RISK MANAGEMENT**

The following requirements are imposed on decisions in the sphere of compliance and risk management of the Company:

- decision-making in the sphere of compliance and risk management shall be carried out in the manner regulated by these Regulations;
- decision-making and decision implementation in the sphere of compliance and risk management shall be carried out in accordance with the division of powers and responsibility regulated by these Regulations.

Restrictions on the Company's policy in the sphere of compliance and risk management:

- Company officials shall take compliance and risk management decisions only within the bounds of their authority and responsibility secured in their job descriptions and Company by-laws.

Restrictions on the permissible risk volume within the scope of the Compliance and Risk Management System shall be set in the relevant standards for the Company's operations.

## **6. IMPLEMENTATION OF THE COMPLIANCE AND RISK MANAGEMENT POLICY**

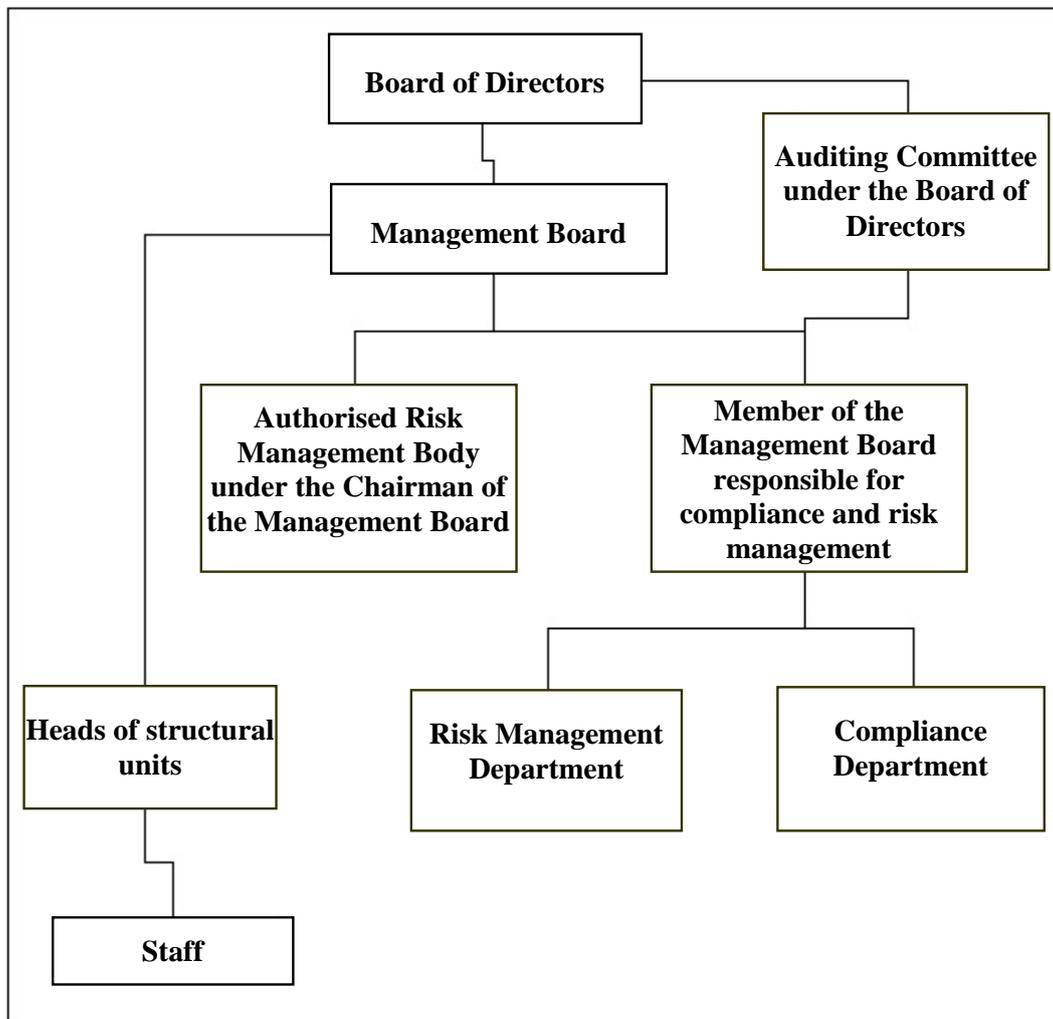
### **6.1. General structure of the Compliance and Risk Management System<sup>[2]</sup>**

The Compliance and Risk Management System of the Company is defined as the aggregate of management subjects, participants and methods.

The subjects of the Compliance and Risk Management System are the Company's risks, irrespective of their place in the classification.

The participants in the Compliance and Risk Management System are:

- Board of Directors of the Company,
- Auditing Committee under the Board of Directors of the Company,
- Management Board of the Company,
- Authorised Risk Management Body under the Chairman of the Management Board,
- Member of the Management Board responsible for compliance and risk management,
- Risk Management Department,
- Compliance Department,
- Heads of structural units of the Company,
- Company staff.



**Fig. 1. Structure of the Compliance and Risk Management System in the Company**

The Compliance and Risk Management System management methods are determined by these Regulations and the Company's standards in the Compliance and Risk Management System sphere.

### **6.1.1. Compliance System (CS)**

The Company's compliance system is orientated on ensuring the operational efficiency of the Company's activities, accurate reporting and compliance with the regulatory requirements by organising control procedures in all material operations of the Company's business processes.

*The subsystem for information disclosure compliance (hereinafter referred to as the SIDC) is an integral part of the Company's compliance system (CS) and fulfills the tasks of ensuring compliance in the sphere of disclosure of financial and other material information provided in the Company's public reporting. The SIDC unites the complex of structural units, by-laws and directive documents, unified rules and procedures regulating the composition of the information, the procedure for gathering, processing and providing it for the purpose of ensuring disclosure of complete and reliable information about the Company and its financial status in reports for external users. The procedures included in the SIDC for gathering and processing information are part of the Company's document flow system. The gathering and processing of information in the SIDC are performed on the basis of the regulations governing the formation of the relevant report documents.*

### **6.1.2. Risk Management System (RMS)**

The risk management system is orientated on raising the efficiency of management decision-making by means of comprehensive and timely identification, analysis and management of the risks associated with achieving the Company's goals. The risk management system includes the aggregate of structural units, by-laws and directive documents regulating the gathering of the requisite data about the Company's risks, their analysis and processing, planning of risk management measures, monitoring and assessment of risk management effectiveness and creation of the necessary information environment.

## **6.2. Functional structure and distribution of powers**

The participants in the compliance and risk management system include:

### **6.2.1. Board of Directors of the Company**

The functions of the Board of Directors of the Company in the Compliance and Risk Management System are:

- approval of the Policy (and amendments thereto) in the sphere of compliance and risk management;
- approval of the Company's risk management strategy;
- decision-making on the effectiveness of the Compliance and Risk Management System;
- organisation of and control over the activities of the Auditing Committee.

### **6.2.2. Auditing Committee under the Board of Directors of the Company**

The Auditing Committee under the Board of Directors fulfils the following functions within the scope of the Compliance and Risk Management System:

- control over the functioning of the Company's Compliance and Risk Management System and preparation of Company Board of Directors resolutions on the effectiveness of the Compliance and Risk Management System;
- identification of material shortcomings in the compliance and risk management procedures, initiation of processes to remedy them;
- elaboration of recommendations of the Board of Directors to improve the Compliance and Risk Management System, the procedures for drawing up the Company's reporting and for disclosing information;
- approval of the sections on risks and the Compliance and Risk Management System in the Company's annual reporting;
- provision for the functioning and management of procedures for disclosing information about the Company's activities;
- keeping top managers informed about material facts that might affect information disclosure;

- making of recommendations to top managers about how information about material facts should be disclosed in the documentation furnished to external users;
- determination of the accuracy and completeness of the preliminary public report containing the disclosed information.

### **6.2.3. Management Board of the Company**

The functions of the Management Board of the Company within the scope of the Compliance and Risk Management System:

- formation of Policy in the sphere of compliance and risk management of the Company;
- formation of the Company's Strategy in the sphere of risk management;
- approval of compliance and risk management standards;
- approval of the prioritised risk register and critical risk owners;
- approval of action plans for managing critical risks;
- provision for achieving the key performance indicators for effectiveness of the Compliance and Risk Management System by introducing the goals of the Compliance and Risk Management System into the corporate financial motivation system.

### **6.2.4. Authorised Risk Management Body under the Chairman of the Management Board**

The Authorised Risk Management Body under the Chairman of the Management Board of the Company is made up of members of the Management Board of the Company and key risk specialists and fulfils the following functions within the scope of the Compliance and Risk Management System:

- approval of the risk tolerance levels and the risk assessment scales;
- prioritisation of the Company's risks;
- formation of critical risk management action plans;
- determination of critical risk owners;
- control over implementation of the Company's critical risk management action plan;
- analysis of the risk management reporting submitted by the Internal Audit and Risk Management Department;
- approval of the annual reporting to the Management Board on implementation of risk management measures within the Company;
- determination of the composition and nature of the information disclosed to interested parties with respect to risk management.

### **6.2.5. Member of the Management Board responsible for compliance and risk management**

The functions of the Member of the Management Board responsible for compliance and risk management within the scope of the Compliance and Risk Management System are:

- management and organisation of the risk management, compliance and audit processes;
- coordination of the activities of the Authorised Risk Management Body under the Chairman of the Management Board of the Company, the Risk Management Department and the Compliance Department with other management bodies, structural units and functional departments of the Company;
- formation of standards in the sphere of risk management, compliance and audit;
- ensuring that the Compliance and Risk Management System abides by the best world practices;
- formation of plans for developing and improving the Company's Compliance and Risk Management System;
- formation of the reporting to the Management Board and the Auditing Committee under the Board of Directors on implementation of measures in the sphere of the Compliance and Risk Management System within the Company;
- approval of the Company management and staff training programme in the sphere of risk management and compliance.

### **6.2.6. Structural subdivisions of the Company responsible for risk management and compliance**

#### ***Risk Management Department:***

- introduction of amendments into Company by-laws envisaging risk management procedures and mechanisms;
- provision of information about critical risks and expenditure on managing them for the purposes of formulating the Company's strategy and budget;
- analysis of outside sources of information regarding the Company's activities, interested parties of the Company and the industry as a whole for the purpose of identifying changes in the Company's business environment and including new risks in the risk register or adjusting existing ones;
- development of a risk management information system (RMIS) for the purpose of automating the gathering and processing of information about risks and providing for its use throughout the Company;
- elaboration of risk management methods and procedures in accordance with the best world practice criteria and approaches;
- gathering, processing and analysis of risk identification information received from structural units of the Company, analysis of in-house documentation and interviewing;

- compilation and adjustment of the Company risk register;
- organisation of risk prioritisation;
- determination of risk tolerance levels;
- consolidation of critical risk management action plans;
- implementation of the portfolio approach to risk management in the form of interaction between risk owners in the process of performing additional analysis of critical risks for the purpose of determining the interconnection between risks and in the process of formation of risk mitigation action plans in order to optimise them;
- development of a risk management reporting system and its review when necessary;
- preparation of the risk management section for the Company's annual reporting;
- consolidation of information about the need for training, elaboration of timetables and programmes for risk management training;
- preparation of reporting to the Management Board on implementation of risk management measures within the Company;
- development of the Company management and staff training programme in the sphere of risk management.

***Compliance Department:***

- elaboration of compliance methods and procedures in accordance with the best world practice criteria and approaches;
- methodological support for the work of structural subdivisions, branches and SDCs of the Company in performance of control procedures;
- performance of checks and assessments of the adequacy of control procedures;
- elaboration and introduction of new control procedures in accordance with shortcomings revealed;
- development of a compliance reporting system and its review when necessary;
- provision of methodological support for Company managers in compiling compliance reports;
- preparation of the compliance section for the Company's annual reporting;
- consolidation of information about the need for training, elaboration of timetables and programmes for compliance training;
- preparation of reporting to the Auditing Committee under the Board of Directors on implementation of measures in the compliance sphere within the Company;
- development of the Company management and staff training programme in the sphere of compliance.

### **6.2.7. Heads of structural subdivisions and branches of the Company**

The main functions of the heads of structural subdivisions and branches of the Company within the scope of the Compliance and Risk Management System are:

- implementation of these Regulations and exercise of relevant control over observance of its provisions in the subordinate structural subdivision or branch;
- identification of the risks of the subordinate structural subdivision or branch;
- implementation of the risk management action plan within the bounds of their terms of reference;
- determination of the needs of employees for training in the sphere of compliance and risk management.

### **6.2.8. Company staff**

The main functions of the Company staff within the scope of the Compliance and Risk Management System are:

- fulfilment of job duties in the sphere of compliance and risk management in accordance with their job descriptions;
- prompt notification of the management of structural subdivisions or branches of any existing or potential errors/shortcomings that have led or might lead to possible losses;
- undergoing training in the sphere of compliance and risk management in accordance with the approved training programme.

### **6.3. Regulatory documents in the sphere of compliance and risk management**

These Regulations are binding on all Company employees and require compliance by and/or adjustment of the Company by-laws in relation to liability for risk management and compliance.

**Compliance standard** regulates the set of compliance procedures and their application within the Company, responsibility for implementation of the procedures, and the methods for assessing the effectiveness of compliance control within the Company.

**Operating and investment risk standard(s)** regulate(s) the processes of risk identification, assessment and analysis, elaboration of risk management measures and exercise of control over effective management of the Company's operating and investment activity risks.

**Acts regulating liability and powers of structural units and collegial bodies of the Company** are: Regulations on the Board of Directors and the Auditing Committee (in relation to compliance and risk management), Regulations on the Authorised Risk Management Body under the Chairman of the Management Board, the Compliance Department, the Risk Management Department, structural subdivisions and so on, orders on distribution of responsibility and powers and job descriptions.

**Acts regulating the work of the subsystems and procedures within the Compliance and Risk Management System** are: Regulations on Information Policy, Regulations on Stock-taking, and so on.

**Rules governing interaction between employees in the process of compliance and risk management** are: Information Disclosure Procedure, Rules on Performance of Audits within the Company by the Compliance Department, and so on.

**Acts regulating accounting and reporting procedures** are: Accounting Policy, Working Chart of Accounts and Instruction for its Application, recommendations on booking individual operations.

---

<sup>[1]</sup> When the Company management adopts a decision to enter international trading markets, the internal audit function will be separated from compliance and risk management in accordance with the principle declared in these Regulations of division of responsibility and the requirements of international standards and exchanges. This principle is not currently being implemented by the Company in relation to internal auditing which remains combined with compliance and risk management.

<sup>[2]</sup> The presented scheme lacks an independent internal audit department (for more detail, see the comment on page 9).