

**APPROVED BY**  
**The BoD of OAO “IDGC of Urals”**  
**Session held on 04.06.2010,**  
**Protocol #70 dd. 07.06.2010**

**The Risk Management Policy**  
**of OAO “IDGC of Urals”**

Ekaterinburg

2010

## Contents

1.	BASIC CONCEPTS, DEFINITIONS AND ABBREVIATIONS .....	3
2.	GENERAL PROVISIONS.....	6
3.	RISK MANAGEMENT STRATEGY .....	7
3.1	<i>RM Goals and Objectives</i> .....	7
3.2	<i>Principles and requirements placed on RMS</i> .....	7
3.3	<i>Approach to shaping risk appetite</i> .....	8
3.4	<i>Priority risk spheres</i> .....	8
4.	RISK MANAGEMENT PROCESS .....	10
4.1	<i>Risk identification and evaluation</i> .....	10
4.2	<i>Elaboration and performance of RM activities</i> .....	11
4.3	<i>Risk Monitoring</i> .....	12
5.	RMS ARCHITECTURE .....	13
5.1	<i>RM Levels</i> .....	13
5.2	<i>Organizational RM Structure</i> .....	13
5.3	<i>Roles and Responsibilities of RMS participants</i> .....	14
5.4	<i>The RMS Information Provision</i> .....	15
6.	REPORTING ON RISKS .....	16
6.1	<i>Regulating documents and standards</i> .....	16
6.2	<i>Protocols and reports</i> .....	16
6.3	<i>Evaluation of RM efficiency and key risk indicators</i> .....	17

# 1. Basic concepts, definitions and abbreviations

**Internal Control System (ICS)** is a whole range of procedures, methods and mechanisms of control, elaborated by the Company's BoD and management to ensure proper financial and economic performance. Internal control procedures are an integral part of the Company's business processes. They are performed either during the business process or prior or following an operation.

## **Internal Control System enables to:**

- Ensure performance during efficient management of the company;
- Ensure observation of legal and regulatory requirements;
- Ensure asset safety;
- Prevent mistakes and violations, reveal them and decrease their quantity;
- Ensure accounting relevance, authenticity, integrity and correctness;
- Ensure preparation of timely and authentic financials.

**Internal control (IC)** is a process aimed at ensuring reasonable guarantee of pursuing the aims of efficient and resultative usage of the Company's resources, asset safety, observance of legal requirements and submission of authentic financials.

**Internal audit (IA)** is a range of activities in evaluating ICS reliability and efficiency, risk management system, efficiency and economy of business process management as well as consulting the Company's management during elaboration of ICS systems and procedures.

**Risk management (RM)** is a process performed by the Board of Directors, senior officers and other employees aimed at revelation, management and control of events that may have a negative influence on the company's objectives.

**Risk Management System (RMS)** is a totality of processes, methods, information systems aimed at the achievement of risk management goals and objectives.

**Risk** is a combination of event occurrence probability and consequences (ISO/IEC Guide 73:2002). For the purpose hereof, a risk (a risk event) is a possible event that may have an influence on the achievement of the Company's strategic and operating objectives in the long run. Risk influence is divided into negative and positive.

**Risk appetite** is the amount of risk that a company can undergo to achieve the aim of increasing its value.

**Risk factor** is an occasion or surroundings bearing a possibility of risk occurrence.

**Risk consequences** are events that are most likely to happen after risk occurrence. Risk consequences are expressed by the influence on efficiency and objective deadlines, financial

result, reputation, reliability of services, human resources and other factors of achieving the Company's strategic and operating goals.

**Probability of risk** is a measure for a possibility of risk occurrence.

**Substantiality of risk** is a measure of risk consequences.

**Risk management** is a process performed by officers and clerks on every management level of the Company and its structural subdivisions, including:

- Risk identification and evaluation,
- Risk ranking,
- Influencing risk within risk appetite

to ensure reasonable guarantee of achieving the Company's strategic and operating goals (COSO ERM).

**Risk owner** is a head of a subdivision which strategic or operating goals are influenced by the risk. A risk owner is responsible for identification, evaluation and monitoring of risk management and is appointed by the Company's CEO.

**Guarantor** is a person responsible for the arrangement of risk management.

**Risk passport** is a document containing all information on a risk.

**Risk register** is a data base containing key information on the Company's risks.

**Key Risk Indicators (KRI)** are quantitative indices of risk (factors).

**Risk coordinator** is a person responsible for coordinating risk management processes within one structural subdivision, in particular, collection and update of information on risk, consulting risk owners on risk management methodology, provision of information to the parties concerned.

**ISO/IEC Guide 73:2002** is a standard of the International Organization for Standardization and International Electrotechnical Commission "Risk Management. Glossary".

**COSO ERM** is a model for risk management in a company of Sponsoring Organizations of the Treadway Commission, widely used in global risk management practices.

**Control procedures** are a range of measures enabling to exclude (decrease) a possibility of risk or to prevent its consequences.

**Internal Control Subjects – the Board of Directors** (Audit BoD Committee), CEO, Department (Directorate) for Internal Control, Audit and Risk Management as well as subdivisions and personnel of the Company and its branches, responsible for internal control, audit and risk management, formalized for them by the Company's internal documents.

**Inspection (audit)** is a controlling activity or research of a situation in certain Company's activities.

**Audit of the Company's business process ICS** is an activity lying in collection, evaluation and analysis of audit evidence, in relation to the ICS of a business process, subject to audit, and resulting in an auditor opinion on the reliability level of process ICS.

**Structural subdivision** is a subdivision of the approved organizational structure of the **Executive Office of the Company (EO)**.

## 2. General provisions

The Risk Management Policy of OAO “IDGC of Urals” (hereinafter referred to as the Policy) determines basic principles of arrangement, implementation and control of the risk management processes in OAO “IDGC of Urals” (hereinafter referred to as the Company). The Policy determines high-priority activities on the arrangement of risk management system.

The present document covers the following spheres:

- Risk management strategy
  - RMS goals and objectives;
  - RMS principles and requirements;
  - Risk appetite;
  - High-priority risk spheres of the Company (ranking).
- Basic risk management processes:
  - Risk identification and evaluation;
  - Elaboration and performance of RM activities;
  - Risk monitoring.
- RMS architecture:
  - Risk management levels;
  - Organization structure of RM subdivisions;
  - Roles and responsibilities of RMS participants;
  - RMS dataware.
- Risk reports:
  - Regulatory documents and standards;
  - Communications, protocols and reports;
  - Appraisal of RM efficiency.

This Policy is based on the best global RM practices, applied by energy sector, and uses statements from the RM fundamentals (COSO ERM, ISO/IEC Guide 73:2002) as well as other generally accepted RM documents.

The document was prepared for officers and clerks on all management levels of the Company, its structural subdivisions, branches as well as other participants of RM processes and parties concerned.

### 3. Risk Management Strategy

A RM strategy consists of goals, objectives, principles, priorities in risk management as well as approaches to the choice of risk appetite.

#### 3.1 RM Goals and Objectives

RM goals and objectives are represented in Table 3.1.

Table 3.1. RMS goals and objectives

Goals	Objectives
<p><b>Provision of a reasonable guarantee in achieving strategic goals</b></p>	<ul style="list-style-type: none"> <li>• Identification and appraisal of substantiality of events influencing the achievement of strategic goals;</li> <li>• Provision of preventive activities on minimization of risk occurrence possibility and negative influence on goals;</li> <li>• Strategic planning in view of risks;</li> <li>• Timely notification of top managers and concerned parties on the presence of threats and possibilities;</li> <li>• Monitoring of activities on risk control.</li> </ul>
<p><b>Asset safety and retaining business efficiency</b></p>	<ul style="list-style-type: none"> <li>• Risk revelation, appraisal and management of business processes;</li> <li>• Provision of information on risks while taking managing decisions;</li> <li>• Formation of risk control matrices;</li> <li>• Creation and management of the KRI system;</li> <li>• Prevention of fraud.</li> </ul>
<p><b>Provision of non-stop energy transmission</b></p>	<ul style="list-style-type: none"> <li>• Shaping of risk reaction programs;</li> <li>• Regulation of risk consequence allocation processes;</li> <li>• Coordination, provision and evaluation of efficiency in timely reaction to emergencies.</li> </ul>

#### 3.2 Principles and requirements placed on RMS

RMS is based on the following principles:

- System approach. All types of risks are managed in all key operations on all levels of the Company's management.
- Responsibility for risk management. One of the objectives for each employee is risk management within his competence, knowledge and available information.
- Cross-functional interaction. The process of interfunctional RM (risks affecting goals of several functions) is based on collegiate resolutions adopted jointly according to information, available for various functions.
- Single information channel. RMS dataware provides the possibility to timely and fully inform decision-taking persons on the risks.

- Separation of decision-taking levels. Resolutions on risk minimization are adopted on various management levels depending on risk importance. The limits for determining decision-taking level are based on the Company's risk appetite.
- Goal tie-in. Risks are managed due to the goals set forth by the Company's strategy as well as goals of certain processes and functions.
- The bottom-up and top-down movement of the risks. For decision-taking, information on risks comes from the lowest levels to the highest ones. Decisions on risk minimization as well as risk management control come from the highest management levels to lower ones.
- RM economic feasibility. RMS ensures RM economic feasibility. Risks are decreased due to economic expediency.
- Control over RM efficiency. RM efficiency is performed by monitoring KRIs, elaborated for each high-priority RM sphere.

### **3.3 Approach to shaping risk appetite**

Risk appetite is a measure of risk that, in the management's (Management Board or MB) opinion, is acceptable for the Company or its branch. This means that risk appetite matches the Company's resources that can be sacrificed in case of risk occurrence. On the basis of the risk appetite the MB takes decision whether to take the risk or to elaborate over its decrease.

Generally, the risk appetite is linked to the possibility to discharge the liabilities by the Company and its branches. This is determined by linking to financial indicators, for instance, EBITDA, net profit, etc. Alongside with financial indicators, the risk appetite can be linked to indicators of transmission quality, for instance, indices of disrupt frequency and average length, index of repeated outages, etc.

According to the principle of decision-taking level separation, there is own risk appetite for each level.

On extraordinary occasions, when the risk appetite level is exceeded, the risk can be taken if measures, taken to decrease it, are not economically feasible or bear more risk. The non-achievement of the risk appetite on "bottom" level does not mean the lack of necessity to decrease the risk, if it is economically feasible or can lead to a positive effect.

The risk appetite is approved for key risks by the MB's resolution.

### **3.4 Priority risk spheres**

Key basis for risk ranking is risk functional domains. To simplify risk ranking we use the risk classifier approved by the Management Board.

All risks are ranked by the following priorities:

- Commercial risks;
- Financial risks;

- Operating risks;
- Exploitation risks;
- Risks of uninterrupted and reliable energy supply;
- Tariff risks;
- Risks in Corporate Governance and Property Management;
- Legal risks;
- Investment risks;
- Risks in organizational development and HR;
- IT risks;
- Security risks.

## 4. Risk Management Process

### 4.1 Risk identification and evaluation

#### Risk identification

Risks are identified on all management levels according to the Risk Classifier approved by the Company's Management Board.

While identifying risks the following information is determined:

- Risk title;
- Risk description;
- Risk sources;
- Risk owner and person providing information on risk;
- Subdivision and branches;
- Key Risk Indicators.

#### Risk evaluation

Risk evaluation is a totality of risk occurrence possibilities and risk substantiality. Risk is evaluated by a 1-year forecast.

**Possibility of risk occurrence** is expert metrics, determined by 5-point scale (see Table 4.1).

Table 4.1. Scale for determination of risk occurrence possibility

Score	Value, %	Interpretation
1 (Extremely low)	1-7%	Event is likely to happen not oftener than once in <b>15 years</b>
2 (Low)	7-20%	Event is likely to happen not oftener than once in <b>5-15 years</b>
3 (Average)	20-50%	Event is likely to happen not oftener than once in <b>2-5 years</b>
4 (High)	50-70%	Event is likely to happen within <b>1-2 years</b>
5 (Extremely high)	>70%	Event is likely to happen within <b>1 year</b>

**Risk substantiality** has two scales: financial and reputational.

Substantiality is determined on the basis of scenario analysis. Each risk has at least three scenarios (pessimistic, optimistic and basic), which are inconsistent, i.e. cannot occur simultaneously. Every scenario is weighted by a conventional possibility in per cent (possibility of occurrence of a certain scenario in case the risk occurred). According to the condition of inconsistency, the sum of such conventional possibilities for the risk should be 100%. Substantiality, expressed in rubles, and reputation influence, expressed in 5-point scale, is determined for every scenario (see Table 4.2).

**Table 4.2. Reputational scale for evaluation of risk substantiality**

<b>Score</b>	<b>Interpretation</b>
<b>1</b>	Risk occurrence will not essentially influence the reputation
<b>2</b>	Risk occurrence will result in deterioration of reputation and insignificant churn
<b>3</b>	Risk occurrence will significantly influence the reputation and cause a moderate churn
<b>4</b>	Risk occurrence will significantly influence the reputation decreasing investment rating and share price by 5-15%
<b>5</b>	Risk occurrence will significantly decrease investment rating and share price more than 15%

Risk substantiality has two metrics:

- Average damage calculated as mathematic expectation of damage distribution (in financial and reputational indicators) on three and more scenarios;
- Value-at-Risk (VaR) is a damage (in financial and reputational indicators) which will not be exceeded with probability of 95%.

Therefore, risk has 1 estimate of possibility and 4 estimates of substantiality: average damage and VaR on two scales: financial and reputational.

## **4.2 Elaboration and performance of RM activities**

RM activities can be divided into 3 categories:

- Risk optimization – procedures affecting the possibility or substantiality of risk. For instance, performance of control procedures, decreasing the possibility of risk occasion.
- Risk transfer – transfer of a risk or its part from one party to another according to a contract. For instance, conclusion of an insurance contract or process outsourcing.
- Risk prevention – termination (or substitution) of processes with a risk, for instance, substitution of inflammable services for flame-proof ones.

RM activities should be provided with the following additional information:

- Person and subdivision responsible for activities performance;
- Terms for activities performance;
- Intervals for activities performance;
- Supplementary budget for activities performance;
- Status of activities performance;
- Actual terms for activities completion;
- Reference to the documents supporting the fact of activities completion;
- Residual risk following activities completion.

### **4.3 Risk Monitoring**

Risk monitoring lies in control over risk level. This is achieved by a regular (quarterly) update of information on risks, RM activities, status of activities completion as well as by monitoring value of the key risk indicators elaborated earlier during risk identification and evaluation.

The KRIs for all Company's subdivisions that monitor and manage risks, are traced by a department of internal control, audit and risk management on a regular basis, depending on the importance of risk and level of decision-taking on risk.

## 5. RMS architecture

### 5.1 RM Levels

The Company's risk management is multilevel.

Multilevel risk management is divided into 2 categories:

- **Multilevel on corporate governance levels** that corresponds to the Company's corporate structure. The Company has 2 management levels:
  - The Company's executive office (EO);
  - The Company's branches.
- **Multilevel on organization management levels** that corresponds to the goals and operating management and is divided into 3 levels:
  - The Company's BoD level (decisions on risks are taken by the BoD);
  - The Management Board level (decisions on risks are taken by the MB or CEO);
  - Linear management level (decisions on risk are taken by the heads of subdivisions).

Each level of the RMS has **decision threshold** which is a threshold risk value, exceedence of which transmits a decision on risk to a higher level according to the following principles:

- Decision for linear management level is shifted to the MB (CEO) level;
- Decision for a branch's CEO level is shifted to the BoD level (CEO of a higher management level)

### 5.2 Organizational RM Structure

Organizational RM structure corresponds to the Company's management levels.

- The coordination of the RM processes, collection of information, consulting of risk owners on RM methodology is exercised by risk coordinators from subdivisions dealing with internal control, audit and risk management.
- Persons, responsible for collection of information on risk (risk coordinators), are designated in the Company's branches.

Risk coordinators in the Company and its branches operate according to single standards and methodologies. For efficient RM on all management levels interaction between risk coordination is regulated by the single Regulations on risk coordinators interaction.

Risk coordinators are accountable to risk coordinators of a higher management level. This enables to promptly exchange information for taking decisions on decreasing risk level on all management levels.

In the Company's branches officers or clerks, partially responsible for risk management, are designated as risk coordinators.

In the Company itself the CEO (Management Board) takes decisions on risk management.

### **5.3 Roles and Responsibilities of RMS participants**

Roles and responsibility are distributed according to the following principles:

- Responsibility for efficient RM as well as for approval of RM budget lies on **the CEO (Management Board)**. Responsibility for efficient RM on lower levels lies on the regional branch directors.
- Responsibility for solving cross-functional RM objectives (executed simultaneously by several functional subdivisions) as well as drafting RM budget lies on **the CEO (Management Board)**.
- Responsibility for timely revelation, risk evaluation, development and execution of activities, risk monitoring lies on **heads of subdivisions** on all management levels. Heads of the subdivisions which aims are directly influenced by the risk are designated as risk owners.
- Responsibility for methodological maintenance and coordination (timely collection of information) of all RM processes as well as for timely and full provision of information on risks incurred by all interested parties (including the Management Board, Board of Directors) lies on RM coordinators (**risk coordinators**) on all management levels.

The efficiency of risk management is supervised by the **Audit Committee (Board of Directors)**.

Table 5.2. shortly demonstrates the distribution of roles and responsibilities of RMS participants.

**Table 5.2. Roles and responsibilities of the RMS participants**

<b>Participant</b>	<b>Role</b>	<b>Functions and responsibility</b>
<b>Audit Committees at BoD</b>	Controller	<ul style="list-style-type: none"> <li>• Supervision over RM efficiency.</li> </ul>
<b>CEOs (Management Boards)</b>	Guarantor	<ul style="list-style-type: none"> <li>• Arrangement of efficient RM within its structural unit.</li> <li>• Approval of budgets.</li> <li>• Approval of MB-level risk registers</li> <li>• Approval of risk registers.</li> <li>• Budget drafting.</li> <li>• Solutions on situations in dispute.</li> </ul>
<b>Subdivisions</b>	Principals, risk owners	<ul style="list-style-type: none"> <li>• Risk revelation and evaluation.</li> <li>• Development and execution of activities.</li> <li>• Timely submission of information on risks and measures to risk coordinators.</li> <li>• Fixation and transfer of information on occurred risks.</li> </ul>
<b>Risk coordinators (Internal Audit Department)</b>	Methodologist, coordinator	<ul style="list-style-type: none"> <li>• Coordination of RM processes.</li> <li>• Training and consulting on RM process methodology.</li> <li>• Support and development of the RMS methodological and regulating environment.</li> <li>• Provision of information to collegiate bodies, taking joint decisions on risks.</li> <li>• Provision of information on risks to the parties concerned</li> </ul>

## **5.4 The RMS Information Provision**

Information on risk is used during decision-taking. This principle means that information on risks, the amount of risks, current and possible measures on risk management is available and can be disclosed upon request (in case usage of such information is well-grounded) to any officer, clerk within their competence.

Information on risks should be kept as a data base using any information platform (including MS Office). A database on risks is a whole range of related information which can be represented as a risk register and as a passport for each risk.

Decision-taking on the level and depth of the RM process automation is at the CEO's (MB's) discretion.

## 6. Reporting on risks

### 6.1 Regulating documents and standards

The RMS regulating framework is based, complies and does not contradict the statements of the present Policy.

The RMS regulating framework is formed for every management level:

- The Executive Office
- The branches.

Table 6.1 demonstrates **compulsory**<sup>1</sup> register of the RMS documentation and its purpose.

**Table 6.1. Compulsory list of the RMS regulating framework**

<b>Document</b>	<b>Purpose</b>
<b>The Risk Management Policy</b>	Basic principles for arrangement, implementation and control over risk management processes.
<b>Risk classifier</b>	Description of risk spheres which can further be specified by detailed information on objects subject to the risks, subjects of risk influence, terms, regulating acts, projects, contractors and other relevant information providing full picture of the risk sphere under review.
<b>The Regulation on Risk Appetite and Decision Thresholds</b>	Formalization of risk appetite, thresholds for separation of risk decision-taking levels.
<b>The Methodological RM Guidelines</b>	Description of approaches and methods for risk identification and evaluation, elaboration of risk management measures.
<b>The Risk Management Standard</b>	Description of terms responsible for risk management procedures.
<b>Reports on risk management</b>	Forms of information on risks from subdivisions as well as reporting forms on risks for the parties concerned.

### 6.2 Protocols and reports

RMS reporting enables to achieve the objectives of risk management and is designed for full and transparent exchange of information on risks and informing persons taking decisions on risks in compressed format.

Table 6.2 demonstrates basic list of reporting documents and their purpose.

<sup>1</sup> The RMS regulating documentation register can be completed with other required documents

**Table 6.2 RMS reporting documents**

<b>Reporting document</b>	<b>Persons filling in the documents</b>	<b>Purpose</b>
<b>Risk register</b>	Risk coordinators	Risk register with a key information on risks
<b>Risk passport</b>	Subdivisions, jointly with risk coordinator (if required)	Document describing all the relevant information on risk. It consists of the following main sections: <ul style="list-style-type: none"> <li>• Information on risk;</li> <li>• Risk management measures;</li> <li>• Occurred risks;</li> <li>• Risk reaction procedures;</li> <li>• Key risk indicators.</li> </ul>
<b>Risk map</b>	Risk coordinator	Graphic description of risk importance level. It is a diagram with a possibility of a risk on X-axis, risk integral metrics of substantiality on Y-axis.
<b>Presentations for the MB, Audit Committee, etc.</b>	Risk coordinator	Presentation materials in MS PowerPoint format containing basic information on risks and the status of risk management process, current and future risk management objectives.

### **6.3 Evaluation of RM efficiency and key risk indicators**

RM efficiency is evaluated on the basis of:

- Analysis of dynamics of risk evaluation change;
- Analysis of integrity and completeness of measures on risk decrease;
- Dynamics of the KRI change.

The KRI is an indicator characterizing a risk factor, but not being its evaluation.

The KRIs are elaborated by the subdivisions, risk owners, and approved by the CEO or MB.

To secure responsibility for target KRI achievement, the KRIs can be fixed as key indicators of manager and subdivision efficiency.

Consistency of the KRI calculation is controlled by subdivision responsible for internal control, audit and risk management.