**ORDER No.**

**Of the Ministry of Finance of Georgia**

**Tbilisi, December, 2011**

**“About Confirmation of the Risk Management manual”**

On the basis of the paragraph 8 of the article 32 of the Law on “Public Internal Financial Control”, I order:

**Article 1.** Confirm “The Risk Management manual” with applied edition.

**Article 2.** This order must come into effect immediately after its publishing.

***Dimitri Gvindadze***

**Risk Management Manual**

1. Risk meaning and its definition;

2. Risk management;

2.1. Risk Management responsibilities;

3.Establish context;

3.1. Define risk management content;

3.2. Define internal and external factors;

3.3. Define risk criteria;

4. Risk assessment;

4.1. Risk identification;

4.2. Risk analysis;

4.3. Risk evaluation;

5. Risk Treatment;

5.1. Risk Treatment Plan

6. Communication and consultation

7. Monitoring and review

**Introduction**

The present document is the methodological guideline for risk management in Public sector and is prepared according to the requirements of the Law of Georgia on “Public Internal Financial Control ” (hereinafter referred to as – the Law).

The manual includes risk management essence and the components inside it considering of which the certain institution elaborates own risk management system, being in accordance with the objectives and activity specificity of the certain institution. The risk management is not performed according to selection, but within the whole institution, at all structural or organizational level. In addition, to receive the best results, the risk management process is desirable to begin as soon as the activities or set task performance begins.

1. **The risk essence and its definition**

The risk is a probability of a result that represents deviation form planned/expected result and affects the achievement of the institution goals.

The risk is defined as the combination of the following characteristics:

1. Probability ofan event;
2. Consequences.

* The probability of an eventis the possibility to come the particulat result, where the frequency of such coming of the result is considered.
* The consequences is an effect in case of certain result The Consequences include four elements:
  + Time
  + Quality
  + Benefit
  + Human and other resources

The combination of probability and consequences define the importance level of the certain risk and give an opportunity to classify the risks according to the priorities considering the goals and objectives of the institution.

The risks should be considered and managed according to the priority: first are the risks with high probability and have the high level of consequences. Every next risk should be considered and managed according to the highest probability of an event and its consequences. Every next risk in the sequence should be risk having lower propability and consequences. In practice, this process is more difficult, because there are risks, with high probability of occurrence, but their consequences are low and/or vice-versa. In such cases the risks should be classified in priorities based on the objectives and goals of the institution to prevent any error (see sample in Table 1).

|  |  |  |
| --- | --- | --- |
| Table 1. | | |
|  | | |
| Probability | High | High priority |
| Consequences | High |
|  |  |  |
| Probability | High | Risks should be prioritized based on the objectives and strategy of the institution |
| Consequences | Low |
|  |  |  |
| Probability | Low | Risks should be prioritized based on the objectives and strategy of the institution |
| Consequences | High |
|  |  |  |
| Probability | Low | Low priority |
| Consequences | Low |

**2. Risk management**

The risk management represents the process of risk identification, assessment and monitoring for the purpose of maintaining the risk at the acceptable level, that has an influence on the achievement of the objectives and goals of the institution and implies measures necessary for risk level reduction.

The risk management is a united, continuous and developing process, in which each employee takes part within the proper competence.

The risk management is one of the important components of strategic management of the institution.

The main goal of the risk management is identification and treatment of risks. It marshals the understanding of the potential upside and downside of all those factors which can affect the institution.

The risk management should address methodically all the risks surrounding the institution’s activities past, present and in particular, future.The managers should provide the formation of the relevant system of risk management and its functioning, and the obligation of the internal audit unit, formed inside the institution, is to assess risk management system and make appropriate recommendations for its improvement.

The risk management should be permanent and perform according to the risk management strategy endorsed by the head of the institution on annual basis.

The risk management assists and enhances the institution, providing the efficient fulfillment of its goals, including:

* The formation of general directions of the institution, giving the opportunity to run the future business of the institution in order and control…
* Improve some of the processes, such as: decision-making, planning and give priorities;
* Facilitate efficient distribution and use of the assets and resources of the institution;
* Uphold and protect the reputation and assets of the institution and their enhancement;
* Develop and improve HR and institutional knolwdge bases;
* Operations optimization and other.

The risk management process is an unity of coordinated and consecutive actions. Its consistent parts depend on the specification of the institution, its objectives and strategy; though the general structure of the risk management process is the same in all the institutions (see Table 2).

|  |
| --- |
| **Table 2.** |
| Risk management process ( according to ISO 31000) |

**1.** Risk Management responsibilities

**a) Responsibility of the head of the institution:**

• Define strategic approach to the risk and the acceptable level of the risk;

• Establish the structure for risk management;

• Understand the most significant risks;

• Manage the institution in a crisis, etc.

**b) The responsibility of the head of the structural unit subordinate to the institution:** • Build risk aware culture within the structural unit;

• Ensure the fulfillment of the recommendations made for risk management improvement;

• Identify and report changes circumstances/risks, etc.

**c) The responsibility of each employee:**

• Understand, accept and implement risk management;

• Report inefficient, unnecessary or unworkable control activities;

• Make reports on losses;

• Co-operate with management on incident investigation, etc.

**d) The responsibility of risk manager (if there is any):**

• Elaborate risk management policy and keep it up to date;

• Document the risk management policy;

• Co-ordinate the risk management and internal control activities;

• Collect information related to risk management and report to the managers, etc.

**e) The responsibility of internal audit unit:**

• Elaborate risk-based strategic and annual plans of internal audit;

• Perform auditing of risk management processes in the institution;

• Assess the efficiency and effectiveness of control activities, etc.

**3. Establish context**

Each institution functions in the certain environment having the influence on the risks accompanying the institution. Consequently, the effective risk management should thoroughly consider the specification of the environment of functioning of the institution which implies as well analysis of the risks related to the institution. Establishing context the definition of such main parameters, in the frames of which the risk managing and definition of relevant format for this process will be possible.

Establishing the contextincludes:

a) Definition of the risk management content;

b) Definition of Internal and external factors;

c) Elaboration of risk criteria.

* 1. **The risk management content**

The definition of risk management content includes set objectives, goals, strategy, scale and parameters, as well as the establishment of the total scale and limits of the risk management process, such as:

* Definition of the processes inside the institution, actions and goals of the actions performed;
* Definition of such decisions that are taken in the process of realization of the goals and functions of the institution;
* Definition of activity time and place of the institution’s business;
* Define the capacity of risk management measures in advance that does not exclude the certain changes in the future, etc.

At the phases of the risk management content formation, the following specific issues may be discussed:

* The role and the responsibility of various structural units of the institution in the process of risk management;
* The interrelation of the certain activities carried out in the institution.

**3.2. Internal and external factors**

At the initial stage of the risk management, the risks should be divided into internal and external factors.

Internal risk is a risk caused by the internal resources, and the external risk is a risk caused by the influence of external factors.

The risk may be divided into strategic, financial, operational and other risks. The risks of such categories might be caused by the influence of internal or external factors, as well as from both factors.

The main internal factors having influence on the risk management activities of the institution are as follows:

* governance, organizational structure, roles and accountabilities;
* The capabilities, understood in terms of resources and knowledge (time, processes, human resources, systems, fund of the institution, technologies, etc.);
* policies, objectives, and the strategies that are in place to achieve them.
* information systems, information flows and decisionmaking processes (both formal and informal);
* Legal acts, standards, instructions and other guidelines used by the institution;
* Form and extent of contractual relationships and others.

The external factors:

* Economic, social, regulatory, cultural, financial, political and other factors that have an influence on achievement of the goals of the institution;
* relationships with, and perceptions and values of external stakeholders(see an example in the Table 3).

|  |
| --- |
| **Table 3. Example of internal and external factors**  **Financial risks**  Foreign Exchange  Credit Rating  Liquidity  **Strategic Risks**  Economical Crisis  Political Decisions  **Operating Risks**  **Hazard Risks**  Qualification of Employees  Reorganization  Service Quality  Recruitment  Employees  Publicity  Assets  Agreements  Natural Events  Legislation  Culture  **Internal Factors**  **External Factors**  **External Factors**  Decision-making process  Management  Cash Flow |

**3.3. Risk criteria**

After the elaboration of the above mentioned internal and external factors of risk management content, the risk criteria should be defined that might be operational, technical, financial legal, social, about protection of environment, humanitarian and other kind of criteria.

Generally, a criterion depends on internal regulatory laws, objectives and goals of the institution as well as the interests, expectations and suggestions of the interested parties.

At the first stage, the general criteria should be elaborated for risk assessment and then to be developed and accomplished in accordance with the selection of technics of risk identification and analysis. The risk criterion should be adequate to the methods of risk category and risk level expression method.

**4. Risk assessment**

After the risk environment assessment, the next phase is risk assessment which is divided into three phases: risk identification, risk analysisi and risk evaluation.

**4.1.Risk identification**

The risk identification is a process in which the risk is found and described in details (for the example see the table 4). It is important that the identification should be the well formulated continuous process covering all risks. Otherwise, the risk management process will not be spread on the non-identified the so called “overlooked” risk and might have a negative influence on the achievement of the institution’s goals. Each institution should categorize risks according to the specifics and objectives of the institution, where the risk causing sources will be seen (for example see Table 5).

The risk identification implies the definition of consequence results that gives an opportunity to avoid maximally the probable negative effect.

|  |  |  |
| --- | --- | --- |
| **Table 4.** | | |
| **The detailed description for the risk** | | |
| 1 | Risk name | * Unique identifier or risk index |
| 2 | Risk bounds | * Qualitative description of events, their size, type, number and others. |
| 3 | Risk category | * Strategic, operational, financial, knowledge management, compliance and others. |
| 4 | Interested persons | * Internal as well as external interested persons and their expectations. |
| 5 | Risk condition | * Importance and probability. |
| 6 | Loss experience | * The similar incidents happened before and the loss experience related to the risk. |
| 7 | Risk tolerance | * Potential loss and financial result of risk influence. * Probability of potential loss. * Purposes of risk control. |
| 8 | Measures in return and controlling mechanisms | * By means of which the risk is coped * Reliability quality of existing ccontrol * Elaboration of procedures for monitoring and analysis |
| 9 | Potential ways to improve | * Recommendations for risk reduction |
| 10 | Elaboration of strategy and policy | * Define responsible person for elaboration of strategy and policy related with risks |

|  |  |
| --- | --- |
| **Table 5.** | |
| **Risk Categories** | |
| **Strategic risks** | This category concerns with long-term strategic objectives of the institution, which may be “harmed” by the following risks, such as political risks, legislative and regulatory changes and institution’s reputation risk. |
| **Operational risks** | This category amalgamates those every-day risks that the institution faces in evryday operations |
| **Financial risks** | This category includes risks and external factors related to the efficient management and control of finances: crediting availability, foreign exchange, interest ratio flow and other current processes. |
| **Knowledge management** | This category includes the risks related to the efficient management of knowledge and control. The external factors of this category should be unauthorized or misuse of the intellectual property, competitive technologies. Internal factors might be improper operation of the system or out flowing of the proper staff/personnel. |
| **Compliance** | This category includes the issues like health and security, data base accessibility, operations regulatory issues. |

**Methods for risk identification:**

* Interview and discussion with the group of presons with different specialization;
* Filling in the questionnaires;
* Analysis of past period events;
* Analysis of existing database of risks;
* Analysis for various potential development of events;
* Systematization and structural analysis of the functions performed by various structures and/or persons of the institution;
* Operational modeling.

**4.2. Risk analysis**

The risk analysis is performed according to the study of identified risk probability and their Consequences, in order to define the ways of their management. Thus, the risk analysis means the identification of such factors, which may have influence on the probability and Consequences of risk happening.

At the initial stage the preliminary analysis is performed that means the grouping and consolidation of the similar risks and exclusion of risks with low-influence consequences (it is worth to mention that exclusion does not mean ignoring, because their acounting/recording was performed at the stage of risk identification).

The next stage is to define the risk level considering its scale. The risk level definition is made not only according to the study of risk probability of occuarence and consequences, but risks interrelation and other factors are considered as well.

The risk level might be acceptable for the institution and is called the Risk Tolerance.

It is also possible to define not any certain risk, but combines risks as well.

The risk analysis might be performed in different ways, depending on the certain risk, scope of analysis, available information, data, resources, etc.

The risk analysis may be:

* Quantitative;
* Qualitative;
* Combined.

***Quantitative analysis***

In case, if there are the quantitative data of risk probability of occuarence and consequences, the best way is to perform risk quantitative analysis. Non quantitative assessment is less reliable, especially during risk happening probability of occuarence assessment.

In cases of quantitative analysis the following methods may be used:

* Probability analysis;
* Influence analysis;
* Computer modeling/simulation;
* Statistical analysis and others.

***Qualitative analysis***

Qualitative analysis is widely spread in public sector, where the result of reporting and influence on the society is very important, which frequently makes impossible or expensive to express risks in numbers. Such kind of analysis is based on personal assessment and in such cases decisions are made on the basis of the experience, knowledge, discussion and intuition of the managers. This type of analysis describes verbally the probability of risk happening and scale of influence (see appendix 2.).

The qualitative may be used:

* In case of non-existence of data and resources necessary for quantitative analysis;
* As the means of risk investigation at the initial stage of the risks analysis;
* When such kind of analysis is enough for performing of the proper analysis and decision-making.

The most known practice is the elaboration of risk matrix in the process of risk analysis, which gives an opportunity to rank and detect risks. The matrix is made by the interrelation of the risk probability and consequences, according to which the risk is rated and categorized (see example in Table 6).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Table 6. Example of risk matrix** | | | | |
|  | | | | |
| **Probability** | High | 3 | 6 | 9 |
| Medium | 2 | 4 | 6 |
| Low | 1 | 2 | 3 |
|  | | Low | Medium | High |
| **consequences** | | |

Where:

|  |  |
| --- | --- |
| **High** | * Financial influence is high; * The influence is important on strategy and operations of the institution; * The interest from the parties is important. |
| **Medium** | * Financial influence is medium; * The influence on the strategy and operations of the institution is moderate; * The interest from the parties is moderate. |
| **Low** | * Financial influence is low; * The influence on the strategy and operations of the institution is low * The interest from the parties is low. |

In the risk matrix sample such risks are underlined (bold) the rating of which is unacceptable and some measures should be taken to reduce or avoid them.

**4.3. Risk Evaluation**

The risk evaluation is a process when the result of the risk analysis and risk criteria are compared.

The risk evaluation means the relationship between assessed i.e. Rated risk and the existing control mechanisms and the acceptable risk level of the institution. The risk evaluation goal is to take relevant measures considering the certain criteria and the objectives and tasks of the institution. The risk evaluation includes three phases:

* **Qualitative description of the control mechanism existing in the institution,** namely, what are the processes, policy and other existing factors aiming at risk neutralization. The assessment of the quality of control mechanism existing in the institution is performed with use of the following terms:

a)Non-existing;

b) Inadequate;

c) Adequate;

d) Strong;

e) Excessive (means the existence of too strong control mechanism, which causes the over-spending of material as well as other resources).

**Risk Charactarization considering the acceptable level of risk,** namely, the risk may be described in such a way: unacceptable, acceptable with necessity of treatment and acceptable. The existence of zero level acceptable risk is also possible (in cases when it is impossible to avoid the risk). The risk is acceptable in cases when it is impossible to treat or when the risk itself is not material and insignificant. In such cases it is not reasonable to spend resources.

The risk criteria, measures for risk acceptable level and other parameters related with the risk (e.g. define acceptability level of the unexpected loss, beyond which the loss will be deemed as unacceptable, but within the defined scopes the loss will be deemed as acceptable) may be formed in the institution.

**The decisions risk treatments are based on the first and second phases of the above mentioned risk evaluation,** namely, the types of risk treatment are: avoidance (e.g. by means of not making the decisions or such measures that cause risk, if the risk may be avoided), take certain type of treatment, reconciliation and monitoring (e.g. the risk is acceptable and it is possible to reconcile with it and to make monitoring in cases when taking certain type of treatment is not practical or is impossible. The reconciliation and monitoring are performed in relation with such risks the level of influence of which is insignificant, but the characteristics may be changed in future) etc.

**5. Risk treatment**

As a result of risk assessment, the decision is made about what kind of treatment is necessary of the risks elicited and what is the most effective strategy.

The goal of the risk treatment is to reduce negative influence of the risks of the institution that is reflected in danger reduction and in achievement of the set goals of the institution completely.

The risk treatment, mainly, include risk control, but beside it we come across to such measures as risk avoidance, risk sharing, risk financing, etc.

Among the risk treatment types the selection of the best one means the comparing of the expenditures of the treatment with the benefit. The risk management value should be relevant to the benefit received as a result of such kind of management.

While making comparison of expenditure and the benefit, the certain environment and circumstances should be taken in consideration. It is important to consider all direct and indirect expenses and benefits (tangible and intangible), to assess them according to the financial or other method. During selection of treatment type political and social factors should be taken in consideration.

If the budget for risk treatment is limited, the risk responsive measures should exactly describe those priorities on which the plan of the risk treatment will be based on. It is important to compare the total expenses of treatment with the benefit received as a result of such measures.

The varieties risk treatment types are given below. They also may be used in the combination.

The four principal types of control below are used towards the most part of the risks. These measures aim at reduction risks to the acceptable level:

* Preventive control
* Correcting control
* Addressed control
* Discovering/tracking control

**5.1. Risk Treatment Plan**

The goal of the risk treatment plan is the documenting of the selected plan including:

* Control activities for minimization of the risk level (activity planning);
* Necessary indices form risk level monitoring, assessment of control systems and for risk treatment;
* Definition of persons responsible for the plan performance;
* Definition of types of necessary resources (financial, human, informational, technological, etc);
* Definition of the result of treatment;
* deadlines;
* Requirements of monitoring and reporting;

**6. Communication and consultation**

Communication and consultation is the permanent process giving the opportunity to the institution to provide all the interested persons with the requested information, share and make available for everyone the issues related to the risk management, such as: risk nature, form, probability, treatment, etc.

During the communication the appropriate information is identified and collected, which should be sent in such a form and in such a period of time, that the persons should be able to perform correctly their obligations.

The consultation is a mutual process of the information transfer (informational connection), communication between the institution and the interested persons about the issues that require the decision-making or definition of the certain direction.

The consultation is a process, having influence on decision-making on the basis of collaboration and not on power. The consultation represents a contribution made in the process of decision-making and not decidion-making itself.

**7. Monitoring and review**

The effective risk management requires permanent review of the structure of the institution and reporting for efficient identification and assessment of the risk as well as for definition of the necessary control mechanisms and for relevant treatment. The monitoring also includes the performance an complienceaudit, in order to determine the possibilities of improvement of the structure and activities of the institution.

Since the organizational environment is being permanently changed considering its internal and external factors, it is necessary to make appropriate reforms in the institution,

The monitoring process should ensure that there are the relevant control activities of the institution’s operation and the existing procedures are clear to everyone to perform.

The monitoring process should include as well:

* Assessment – at what extent are the taken measures adequate to the expectations;
* Checking the correctness of the implemented procedures for assessment and received information;
* Assessment, if the fild knowledge and experience is useful for better decision-making and improvement the quality of risk identification, its future evaluation and managament, etc.