## Guidelines for establishment and implementation of risk management in public sector entities

**Introduction**

Aim of the guidelines is to determine a framework for establishment and implementation of unique process of risk management for all public entities.

Guidelines are intended to assist in establishment of this process, to managers in public sector as well as to other employees because this process refers to every individual in the subject.

Efficient risk management will strengthen existing management structure especially in planning and decision making process which will contribute to develop risk management process as standard, widely accepted concept and as integral part of management which will assist in optimal usage of public resources from national and EU funds.

Efficient risk management creates good basis for better decision making process and increase of efficensy as well as for better anticipation and optimal usage of available resources and contribute in strenghtening confidence in public sector management system.

The guidelines include:

* risk management as a part of internal financial control with special emphasis on:
	+ concept of the risk and purpose of risk management, accountability of head of subject and
	+ head of organizational units for risk management and
* main activities of the risk management process

Public sector entities may elaborate proposed framework for establishment and implementation of risk management process more thoroughly depending on task complexity and entity tasks and especially in regard risk identification, using different methods for risk determination such as developmenent of special questionnaire for risk determination, reporting form, an overview of the main risk groups and areas which should be considered in determination of potential risks.

Glossary (Annex 1) is integral part of Guidelines which will assist publics sector entities to better understand the terminology in the field of risk management.

**Risk management as a part of the system of internal financial control**

In accordance with the system of internal financial control in the public sector (“Official Gazette of Montenegro”, No. 73/08, 20/11 and 30/12) system of internal financial controls in public sector consist of financial management and control, internal audit (system of internal controls) and Central Harmonization Unit.

System of internal control in public sector is system of financial and other controls which consist of organizational structure, methods, procedures and internal audit this system is determined and implemented by head of the entity in order to have successful management and accomplishment of task on transparent, correct, economical,, efficient and effective way.

Financial management and control as a part of the system of Internal Financial Control is system of internal controls which is determined by head of entity who is responsible for this system which should ensure reasonable assurance in achieving its goals and budget funds are used properly, economically, efficiently and effectively;

Financial management and control shall be implemented in accordance with internationally accepted standards for internal control using the following interrelated elements:

* control environment
* **risk management**
* control activities
* information and communication
* monitoring and evaluation of system

In order to establish and develop an effective system of financial management and control in public sector in Montenegro it’s necessary to establish and implement the risk management process which is based on COSO framework for risk management and is upgrade of COSO internal control model.

In accordance with the law risk management is the process of identification, assessment, monitoring and control of possible circumstances which may affect the achievement of established objectives of the entity. It involves the introduction of effective ex ante controls in order to reduce risk at acceptable level (a reasonable assurance) which will contribute to achieving the objectives of the entity.

For all entities in system of implementation of EU pre-accession assistance program risk management methodology was developed and each employee in his/her daily work recognize risks which threatens achievement of objectives. Employee should report in a special form about these risks person responsible for risk management and who keeps risk register.Twice a year, on meetings with heads of risks actions for eliminating and reducing riks are determined from risk register.

Experience gained in risk management in managing EU pre-accession funds may help in development risk management process for national funds to ensure unique/ harmonized approach in development of methodology.

**The concept of risk and risk management purposes**

In accordance with article 4 paragraph 1 point 1 of PIFC Law, risk is possibility of occurrence of events which may adversely affect the achievement of objectives of entity.

Risk can also be defined as a threat to successful achievement of goals or anything that represents threat to achievement of goals, programmes or services to citizens is considered as risk.

Missed opportunities for goals achievement are also considered risks.

The risk can occur in different categories/types such as financial risk, projects risk, risk related to services we provide, risk associated with certain interested parties, missed opportunity risk, failure to comply with policies risk, reputation risk, security risk.

There is no definite list of all risks which may affect the achievement of objectives of the entity. However, based on risk definition there may be following categories of risk:

* everything that represents threat to achievement of entity objectives, programmes or services to citizens;
* everything that can harm entity reputation and public confidence in its work;
* insufficient protection of misconduct, abuse, malpractice, damage or low value for money;
* non compliance;
* Inability to react or to manage the changing circumstances in a manner that will prevent or minimize the adverse affects of changes in delivery of public services.

If public sector entities have not established effective system of management of such risks, they may find themselves in situation to spend large amounts of funds for elimination of consequences.

Benefits of establishing and implementing the risk management systems are:

* **Better decision making** - All decisions have a certain level of uncertainty and risk management helps managers to comply their decisions with realistic assessment of planned activities..
* **Increasement of efficiency -** Accepting the risk based approach subject can better decide on how to improve system, allocation of resources and achieving a better balance between acceptable risk levels and cost control.
* **Better forecasting and efficient usage of available resources –** Allows identification of key risks that entity faces and proper allocation of limited available recourses for adequate treatment of identified risks.
* **Strengthening confidence in leadership (management structure) –** Risk management is an essential part of management process in each subject which improves planning process by emphasizing key processes and risks which may affect achievement of process objectives and entity goals.
* **Development of positive organizational culture –** Development of organizational culture which won’t create aversion to risks.

It is important to emphasize that risks are inevitable in everyday business and each subject in public sector is obliged to take action to reduce risk to acceptable level. Risk management process is set of activities that require specific human, time and financial resources and whose starting point is goal result risk register and where is possible action plan or report of risk management.

After the establishment of the risk management process and encourage the development of a culture of risk management and document the most significant risks (risk register), head of the entity will adopt strategy of risk management.

**Risk management – responsibility of management structure**

In accordance with article 13 of PIFC law head of entity is responsible for determination of entity objectives, preparation and implementation strategic and other plans and programmes for objectives achievement as well as identification, estimation and management of risks which may threaten objectives achievement and introduction of appropriate controls for risk management in line with this law and international standards of internal control.

Heads of organizational units at different management levels are responsible for subject objectives achievement in line with delegated authorities and responsibilities within their competences and for risk management.

Risk management is among other things a tool to assist management to estimate changing circumstances and to react on them. Risk management is not separate activity but rather part of regual activities of the head of the entity and head of organizational units which are responsible for finance and human resources management.

CHU will support entities in establishment and development of risk management process by organizing trainings and will monitor implementation of activities.

In order to establish adequate system of risk management head of entity should:

* determine employee responsible for coordination of establishment and implementation of risk management process at entity level and
* **Determine obligation to establish Risk Register at entity level and Risk Register at organizational units level.**

Person responsible for coordination of establishment and implementation of risk management process should:

* inform other heads of units in cooperation with CHU on need of establishment risk management process in entities,
* encourage risk management culture and to help heads of units in effective risk management through raising awareness on importance of risk management
* start activites to introduce risk management process and to set deadlines for certain activities in cooperation with heads of organizational units,
* prepare report on risk management in entity

Person responsible for coordination of establishment and implementation of risk management process in coordination with heads of organizational units should ensure establishment and implementation of risk management process at organizational units level.

**Heads of organizational units** must ensure establishment and implementation of risk management process at level of their organizational units in a way that is possible to:

* identify and evaluate risks in the most important business processes and activities in relation with strategic,operational plans and business processes under organizational unit competences
* evaluate probability of risk occurrence and its impact,
* determine risk responding ways,
* document risk data in Risk Register of organizational units ( it is suggested to have between 10 and 15 most important risks in these Risk Registers),
* report about risks.

A great help in establishing this process may be adopted Books of procedures in which important business processes and activities implemented in organizational units are described and which consist of documentation on financial and other transactions – audit trail from start to end, persons responsible for implementation, way and deadlines for implementation of specific processes and activities.

It is important to mention difference between activities for establishment of risk management process in which person responsible for coordination of establishment and implementation of risk management process and activities related to risk management process in which all heads at all levels of management are responsible.

**Glavne aktivnosti u procesu upravljanja rizicima**

Key stages of risk management:

1. **Identifying risks**
2. **Assessing Risks – Risk Analysis and Evaluation**
3. **Addressing Risks**
4. **Reviewing and Reporting Risks**

****

## Risk identification

Head of the entity is responsible for the identification and analysis of key risks that may affect ability of entity to achieve goals. Risk identification is done in relation to the targets set for all business processes and is implemented during process of entity annual budget planning.

To manage risk, entity should know risks that it faces and to evaluate them. Risk identification is first step.

Identification and risk analysis in the entity is done at entity and organizational unit level taking into account:

* determined goals (strategic, annual and operational)
* legality of operations,
* cost effectivnes, effectivnes and efficiency
* reliably and timely reporting
* protection of resources in case of abuse,
* internal and external information (internal audit, European Commission, the European Court of Auditors)
* the risk occurrence and their impact
* any other information that indicate internal or external risk

Risk identification can be divided into two separate phases. These are:

* initial risk identification (for subject that previously hasn’t identified risks in a structured manner, or for new subjects, or perhaps for new projects or activities within the subject);
* continuous risk identification, which is necessary for identification of new risks which have not previously appeared, changes in external risks, or risks which previously existed and are now non relevant for entity ( this should be routine in business).
	1. **Methods for risk identification**

For determing risks two approaches are usually used:

The first approach is top down approach, where the highest hierarchical level considers risk related to strategic objectives (general and specific objectives).

The second approach is bottom-up approach which includes all organizational units of the entity which review annual activities and business processes and assess the risks.

These two approaches are not mutually exclusive. On the contrary, their combination in risk determination process is desirable because it makes easier risk determination at entity and its organizational unit’s level. In which way risk determination will be organized it depends on specifities of subject. It should be taken into account that the most entities have adopted Book of procedures with description of key business processes.

There are several methods for risk identification but following are mostly used:

**Previous experience**

Data from previous period which is kept by subject or available from other sources are useful for determing the frequency of occurrence and impact of adverse events. This information must be reliable and comprehensive as much as possible. It includes data and analysis

on the implementation of the plans (strategic, operational and financial documents) as well as internal audit reports.

**Using checklists - Questionnaires**

Heads of organizational units prepare their own self-assessment questionnaires. Each risk is considered in relation on previously prepared checklist. Checklists should be regularly updated to make them relevant for operational areas considered.

**Joint workshops – “Brainstorming”**

Risks identification can be successfully done by organizing workshops throughout entity, where participants (employees and heads) with different experience and knowledge approach the problem differently. It is important that participants consider risks in relation on common set objective. This is an effective method, because exchange of opinions leads to best solutions.

* 1. **Risk description**

Risk description is the end of risk identification process and start of risk assessment process.

Identified risks should be described in such a way that’s clear from their description about event, its cause and possible consequence. This is important because risk shouldn’t be perceived differently by different persons.

|  |
| --- |
| **Objective: Implement a new information system that will improve the recording by the end of 2014.** |
| **Description of risk** | **Comment** |
| **Example 1.**Failure to implement new information system for improvement of recording by end of 2014. | **NOT GOOD:** This is simply opposite of entity objective. |
| **Example 2*.*** Insufficient number of employees  | **NOT GOOD:** Do not provide any information about potential impact on activities/objectives or exact cause of risk. |
| **Example 3*.*** Lack of competent staff may cause delays in implementation | **BETTER:** Impact on objective is mentioned but it is not clear enough. However there is no information about risk cause. |
| **Example 4*.*** There is a risk of significant delays in introduction of new project (estimated 10-12 months) because of lack of trained staff. This is partly due to insufficient training of employees. | **IDEALLY:** There is quantified assessment of potential impact on objective. Cause is identified as well. |

**Risk identification approach**

Risks can be categorized as external (political, economic, natural disasters, citizens) and internal (deadlines, employees, qualitative, technological and operational). Because all risks are not threat to entity, each area should be ranked as: insignificant, significant, very significant and disastrous in terms of probability of appearance and impact.

|  |
| --- |
| **Risk Category** |
| **Risk Category** | **Example of risk description** |
| **EXTERNAL RISK:** | Entity can not influence these risks, control measures can be implemented  |
| Political | Changing priorities, objectives, support |
| Natural disasters | Earthquake, floods |
| Legislative | Adoption of legislation which affects stability and operations of entity, mission, objectives |
| **INTERNAL RISK**: |  |
| Reputation | The entity must ensure the quality of public services to its customers  |
| Operating | Employees, competence |
| Financial | Insufficient funds, inadequate planning |
| Informational Technology | Reliability of operation and protection of information is crucial to entity operations |
| General | Compliance with regulations, protection of resources, effectiveness, efficiency, reputation |

1. **Risk assessment**

Once risks are identified they must be assessed in order to rank, identify priorities and provide information to make decisions about what risks to which they should focus.

The methodology for analysing risks can vary, largely because many risks are difficult to quantify (e.g. reputation risks) while others lend themselves to a numerical diagnosis (particularly financial risks). For the former, a much more subjective view is the only possibility. In this sense, risk evaluation is more of an art than a science. However, the use of systematic risk rating criteria will mitigate the subjectivity of the process by providing a framework for judgments to be made in a consistent manner.

General risk ranking is done on the basis of the conclusions drawn in the analysis of general control environment, inherent risks and measurements in terms of impact and probability, which includes employees of the organizational units. Assessment and proposed activities to bring to the court on the basis of individual circumstances.

The risk is analyzed and assessed taking into account the probability of occurrence and potential consequences or effects on the subject.

The risk must be assessed without considering the measures already adopted for its control at an acceptable level, which means that at this stage assesses inherent risk, without taking into account the existence of any form of control.

**Inherent risk** is the risk that in the absence of control and factors that mitigate the risks (risk level without established controls)**.**

Risks are being assessed based on impact and probability.Rizici se procjenjuju na osnovu uticaja i vjerovatnoće.

**Impact** is the evaluated effect or result of a particular outcome actually happening

 An example of measuring a risk Impact is delivered here below.

|  |  |  |
| --- | --- | --- |
| **Rating** | **Ranking Impact** | **Description** |
| 3 | High | Disruption of all essential programs/servicesLoss of major assetsSerious environmental damageDeathSignificant loss of public trustPublic outcry for removal of Minister and/or departmental official |
| 2 | Medium | Disruption of some essential programs/servicesLoss of assetsSome environmental damageSerious injurySome loss of public trustNegative media attention |
| 1 | Low | Schedule delays to minor projects/servicesLoss of assets (low value)Temporary environmental effectFirst aid treatmentSetback in building public trustSome unfavourable media attention |

**Probability** is the evaluated likelihood of a particular outcome actually happening (including a consideration of the frequency with which the outcome may arise). For example, major damage to a building is relatively unlikely to happen, but would have enormous impact on business continuity. Conversely, occasional personal computer system failure is fairly likely to happen, but would not usually have a major impact on the business.

An example of measuring a risk Probability is below.

|  |  |  |
| --- | --- | --- |
| **Rating** | **Probability** | **Description** |
| 3 | High | The event is expected to occur in most circumstances |
| 2 | Medium | The event should occur at sometime |
| 1 | Low | The event occurring is unlikely |

 **2.1. Risk Ranking**

The overall risk ranking is derived from consideration of the conclusions reached in the analysis of the general control environment, the inherent risk and the measurement in terms of impact and likelihood.

The risk ranking will be identified following the intersection of the impact and likelihood.

Overall risk is the combination of impact and likelihood, according the chosen method. Assessment and proposed action must be made according to individual judgement of circumstances.

The categorization of high/medium/low level of risk results in a *“3\*3” risk matrix* that is shown below.

All identified risks must be assessed in relation to the same scale and criteria .

Risk assessment is a subjective evaluation of risk in which assumptions and uncertainties are clearly considered and presented . Part of the difficulty in managing risk, which is the measurement of both the size of the related risk assessment - Impact ( possible loss ) and probability ( that the event will occur ) may be difficult to measure . There is a possibility of error in the measurement of these two concepts . The risk of large potential losses and little prospect of events , often treated differently than a small potential losses and high probability events . In theory , both are almost the same priorities for the response , but in practice it is difficult to implement when you are faced with a lack of resources , especially time , in which to carry out the risk management process . Financial decisions , such as insurance , express loss in monetary terms .

It is important to note that leadership can be considered as unacceptable some risks (death , corruption , etc. . ) , Even though the impact and / or probability of medium or low. Such risks can be ranked on the basis of the decision , not the calculations during the entire process of risk assessment .

The consequences of risk occurrence:

• are not important,

• are important,

• Very important

• catastrophic.

Impact of Risk:

• negligible,

• significant,

• very significant,

• catastrophic.

Showing results will give an overview of risk prioritization from the highest to the less significant is the exposure to risk and subject to risks.

1. **Addressing risks**

Addressing risks is considering possible measures that may affect the acceptability of risk.The purpose of the addresing risks that the uncertainty is turning in favor of the subject, limiting the threat and use of the opportunity provided. Any activity that the entity is taking in terms of addressing risks is part of what is known as "internal controls. "Managers make decisions about addresing risks.

In addition to consideration of the best addressing risks, it is considered to occur when there is the opportunity to exploit the positive impacts that occur there are cases that offer positive opportunities, while at the same time do not make threats.

Reduce the probability and impact will be selecting the appropriate addressing risks. In this regard. There are several ways to addresing risks as follows:

* 1. **Tolerate the risk**

The exposure may be tolerable without any further action being taken. Even if it is not tolerable, ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit gained. In these cases the response may be to tolerate the existing level of risk. This option, of course, may be supplemented by contingency planning for handling the impacts that will arise if the risk is realised.

* 1. **Treat the risk**

By far the greatest number of risk is dealt with in this way, which means that they take actions and make decisions in order to reduce the probability of occurrence and / or impact of the risk.

The purpose of treat the risk is to continue with their activities where the risk arises, while taking actions (control) in order to keep risk at an acceptable level.

The actions that the entity is doing to treat the risk is actually **control activities**.

It should be noted that in most cases the risks can not be completely removed and that each activity contains within itself the potential risk, and control were rated as effective only provide reasonable assurancethat the objectives set are achieved.

**Control activites**

In accordance with the PIFC Law shall be established with the aim to reduce a risk to an acceptable level, received written policies and procedures.

There are different divisions of the control activities in the context of risk management is one of the divisions may be as follows:

### Preventive – designed to prevent the occurrence of inefficiencies, errors or irregularities. These cannot guarantee that the controlled factor will not occur, but they do reduce the chance of it occurring.

### Examples include segregation of duties and authorisation controls.

### Detective – designed to detect and correct errors, inefficiencies or irregularities. They may not give absolute assurance since they operate after an event has occurred or an output has been produced but they should reduce the risk of undesirable consequences as they enable remedial action to be taken. Detective controls are most effective when they form part of a feedback loop in which their results are monitored and used to improve procedures or preventive controls.

###  Examples include post payment confirmation, stock verification and bank reconciliations.

### Directive controls - designed to cause or encourage activities and events necessary to achieve the objectives. One direct a particular process in the desired direction, and ensure the achievement of the objective to be achieved (zakoniska regulations, plans, procedures, resources required to achieve the target).

### Examples include clearly defining policies, setting of objectives and appropriate staff training and adequate staffing

### Corrective controls are designed to correct errors that have been detected.

### Examples are contingency or disaster recovery planning.

### In practice, the above categories of control may not be clearly distinguished and a single control may operate to cover two or more functions. Supervision, for example, covers all four types. Well organised and managed corrective actions and processes are, obviously and logically, also necessary when control weaknesses and failures occur.

 **3.3. Transfer the risk**

For some risks the best response may be to transfer them. This might be done by conventional insurance, or it might be done by paying a third party to take the risk in another way. This option is particularly good for mitigating financial risks or risks to assets. The transfer of risks may be considered to either reduce the exposure of the organisation or because another organisation (which may be another government organisation) is more capable of effectively managing the risk. It is important to note that some risks are not (fully) transferable – in particular it is generally not possible to transfer reputation risk even if the delivery of a service is contracted out. The relationship with the third party to which the risk is transferred needs to be carefully managed to ensure successful transfer of risk.

 **3.4 Terminate the risk**

Some risks will only be treatable, or containable to acceptable levels, by terminating the activity. It should be noted that the option of termination of activities may be severely limited in government when compared to the private sector; a number of activities are conducted in the government sector because the associated risks are so great that there is no other way in which the output or outcome, which is required for the public benefit, can be achieved. This option can be particularly important in project management if it becomes clear that the projected cost / benefit relationship is in jeopardy.

**Risk registar**

The risk register is used to document the results of risk management and monitoring of the proposed measures .

The purpose of the risk register is to provide all the key information about the risks of the enterprise.

The risk register is an internal document that contains :

• Description of risk

• Category of risk

• Assessing the impact and probability

• Review of existing controls

• Responding to risks

• Responsible persons

• Deadlines for implementation

Head of organizational unit completes a risk register for their RTK unit and sends the same person responsible for the establishment and implementation of the risk management process , which checks the completeness of the description and prepare it for submission to the head of the subject. Upon approval , the risks that can accept input in the form of risk register

As the environment and goals change, the risks themselves are changing , and so and risk register must be regularly discussed and accordingly the same date.

The risk register is reviewed at least annually by the head entity and the top management or the proposal of the head of the organizational unit , the person responsible for the FMC , the person responsible for the establishment and implementation of risk management and internal auditors to check whether the planned measures to mitigate risks taken and whether achieving the expected results.

Example Risk Register is an integral part of these Guidelines (Annex 2 )

1. **Risk monitoring and reporting on risks**

The process of risk management is a continuous process that needs to be constantly subject to periodic reviews. This will ensure that the risk register is updated, taking into account the constant changes in the environment, changes in goals, recognizing the emergence of new risks, while others disappear or become less significant in terms of priorities.

Risk management is assessed and it is reported for three reasons:

• to monitor whether the changing risk profile;

• to gain assurance that risk management is effective,

• and to identify when the further action is necessary.

The process of risk monitoring should be established to consider whether the risks are still there, whether they appeared new risks, whether the likelihood and impact of risk change and to izviještavalo of significant changes which are adapted to the priorities of risk, and to ensure the effectiveness of control. Furthermore, the overall risk management process should be subject to the regular inspection to ensure that it remains effective and isti. Review of risk and review of risk management processes that are different and one can not serve as a substitute for the other.

A large number of tools and techniques available to help achieving the examination process:

• Self-assessment of risk is a technique that has already been mentioned in the identification of risk. It also contributes to the review process. Self-assessment of risk results are communicated in the process of maintaining the risk profile of the level of the whole subject. (This process is also sometimes referred to - "control and risk self-assessment");

• "Management Reporting" requires that managers at different levels of the enterprise reporting "up" (usually at least once a year for the financial year, and if necessary, quarterly or semi-annually) of what they did to the risk and control procedures updated and adapted to the circumstances within the area for which they are responsible. This process is in accordance with the Self-assessment of risk . Managers can use the Self-assessment of risk as a tool on which to base the preparation of their management reports.

In addition to these formal resources, individuals, work groups and teams should constantly take into account the risk issues faced in the work they do.

The work of internal audit provides an important, independent and objective assurance on the adequacy of risk management and the adequacy of controls and management. Internal audit can also be used by management as an expert internal consultant to assist in developing strategic risk management entity. It has a broad overview of a series of activities undertaken by the entity and will take some form of assessment to support their planning systems and processes will be reviewed. However, it is important to note that the internal audit is not a substitute for responsible risk management, nor a substitute for the internal built-in review system that performed by employees who have executive responsibility for the achievement of organizational goals.

 organizacionih ciljeva.

Procedures for reporting the results of this process should develop each subject .

**The report** should include an overview of the activities undertaken in the process of risk management and review of significant risks in risk registers organizational unit of the subject .

Heads of organizational units are also required to prepare an annual report on activities related to risk management , which will be the basis for the preparation of **the consolidated annual report on the level of the subject** . The report should include a summary of the significant risks and their impact on the achievement of the objectives of , and information on the actions taken to prevent and mitigation , as well as the risks to which they could not operate as planned . In the preparation of this report may also participate in the person responsible for the establishment, implementation and development of financial management and control .

It is necessary to establish means of communication and exchange of information on identified risks at all levels and among all employees of the entity. This may include : dissemination of results of risk assessment within each organizational unit , as well as a summary of the consolidated annual report on risk management .

Part of the report relating to the activities undertaken to establish a risk management process in the subject will be an integral part of the annual report on internal financial control which shall be submitted to CHU of the Ministry of Finance, and all other information, including information on the most significant risks remain in the subject .

**Conclusion**

Risk management is a continuous process and an integral part of daily management . However, the process needs to be systematic and structured development , especially in terms of developing a unified approach to the level of public sector entities , the introduction of risk management in planning and decision making, as well as to develop a culture of risk management.

In order to ensure successful implementation of risk management in the public sector entities must take steps to :

• ensuring the work environment that will support the establishment of risk management,

• the acquisition and improvement of skills of risk management,

• Establishing effective communication about the risks and activities undertaken for this purpose.

For effective risk management is necessary to create and maintain a work environment that offers support in order to:

• Providing support to the highest level of management,

• creating an organizational culture that will create an aversion to risk and which will

the reporting of risk considered positive and that will give you enough time and resources to raise awareness and develop skills of risk management.

CHU in cooperation with public sector entities hold training workshops on risk management aimed at developing the skills of risk management.

Given that the risk management process at the beginning of the establishment, it is important to provide efficient communication of risks to all employees to be familiar with.

GENERAL DIRECTOR

Mrs. Ana Krsmanović

**Annex 1- GLOSSARY**

|  |  |
| --- | --- |
| **Brainstorming/****Joint workshops** | The method of collecting non-critical opinions of different groups, often used for risk identification and assessment of the level of one organizational unit. The approach is based on the fact that different people with different experiences and knowledge in the different approaches to the problem. |
| **Objective**  | The result of that entity wants to achieve, and the desired future state, whose results are expected in a specified period. One of the divisions may be the strategic goals, annual goals and objectives related to operational plans, programs and business processes.  |
| **Objective of managing process**  | "Reduce the level of uncertainty that could be a threat to the success of the business risk." |
| **COSO**  | Committee of Sponsoring Organisations of the Treadway Commission**-**(COSO) - National Commission for falsified financial statements (known as the Treadway Commission), announced in 1992. document entitled Internal Control - Integrated Framework, which defines internal control as "a process implemented by the board of directors, management and other employees of the enterprise, designed to provide reasonable assurance regarding the achievement of objectives" and compared it to four categories: compliance with applicable laws and regulations, the reliability of the finance and management reporting, effectiveness and efficiency of operations.The purpose of this document was to code management raise awareness on the need for internal control activities as important components of business management.Risk management is established and developed on the foundation of the COSO framework for risk management, which is an upgrade of the COSO internal control model.  |
| **Detective contols** | Designed to identify and correct errors, defects or irregularities. They can not give a completely convincing as acting upon occurrence of the event or after the outcome has already been created, but it would reduce the risk of unintended consequences because they allow preduzmanje additional activity. Detective controls are most effective when you are part of the feedback circuit which monitors their performance and are used to improve procedures or preventive control.Examples of these controls include checking after payment, verification of inventory and reconciliation with bank statements.  |
| **Directive controls**  | Designed to cause or encourage activities and events necessary to achieve the objectives. Guide the process in the desired direction.Examples include clearly defining policies, setting of objectives and appropriate staff training and adequate staffing. |
| **Efficiency**  | A requirement that a certain degree of realization of the targets achieved with the least use of available resources, and the greatest rationality.It represents the realization of an economic objective with minimal cost, effort or loss. To become effective, you have to be organized and systematic."Doing the right things in the right way" (effectiveness)Efficiency is defined as the correct operation, where the way the procedure. |
| **Effectiveness**  | It is understood the request to make the first selection of the right target, and then using available resources achieve maximum realization of the targets.Be "effective" means of producing it for what the system is and established. "Doing the right things, ie. choose the right goals "(efficiency)Effectiveness is an important result.  |
| **Economy**  | Reducing the cost of resources used in the performance of someactivities to a minimum, while ensuring adequateQuality.Minimizing the cost of resources used to achieve planned results related to the specific activity (taking into account the corresponding quality of results). |
| **Inherent level of risk** | The level of risk in the absence of control and factors that mitigate the risks (risk level without established controls). |
| **INTOSAI**  | International Organization of Supreme Audit Institutions  |
| **Treat the risk** | Business decision on non-inclusion or to withdraw from risky situations. |
| **Mission statement**  | A statement indicating the main reason for the existence and activities of the organization, consisting of areas of work, organizational values ​​and goals, that is why institutions exist, and is governed by the regulations. |
| **Control**  | Control is any activity undertaken by management to manage risk and increase the likelihood that the objectives achieved, and measures that will reduce or eliminate the impact of risk. |
| **Control activities**  | Control activities are established to achieve the objectives to reduce risk to an acceptable level, the application of written rules, principles and procedures.In the context of risk management control activities can be divided into Standard, preventive, detective andcorrective. |
| **Corrective controls** | Designed to correct errors that were found.In implementing the corrective actions necessary to determine the cause of the problem, prescribe the manner of correcting errors and modify the system.Examples are correcting entries, fire employees found to have a misuse of business authorities, planning for the contingency planning or for the purpose of disaster recovery.In practice, these types of control can be clearly separated from each other, and a control can be operated sa as to cover two or more functions. For example, monitoring covers all four types of control. |
| **Critical risks** | Risks that the entity is considered unacceptable, for example, would threaten the achievement of the key objectives of the entity, if it can cause harm to stakeholders (citizens, the Government of Montenegro, the European Commission, other entities, etc.)., If the result of the risk of injury law and regulations, if it can cause significant financial loss if you question the safety of employees or if in any case seriously affects the reputation of the subject. |
| **Methods of risks identification**  | Risks can be identified in different ways: using data from the previous period, to hold joint workshops, using special questionnaires and conducting interview |
| **Operational objectives** | Determined on the basis of the strategic objectives, the narrower the scope, the short-term are determined by the desired or expected results of lower organizational units or individual business processes. |
| **Risk description**  | Risk description is of the process completion of identifying risks and begin the process of risk assessment. Before the risk assessment should be clearly formulated, and describe identified risk, taking into account the main cause of risk (which is the main problem) and the potential consequences of risk (impact on goals / activities). |
| **PIFC (Public Internal****Financial Control)** | The system of internal controls in the public sector is a system of financial and other controls, which includes the organizational structure, methods and procedures and internal audit, established and implemented by the head of the subject, with a view to the successful management and accomplishment of tasks subject to transparent, orderly, economical, efficient and effective manner.The system of internal financial control in the public sector are: financial management and control, internal audit and CHU - central harmonization unit. |
| **Contingency planning** | The plan of action in case of adverse events of small probability and high impact action on the subject (e.g. loss of electricity or breakdown of the server). The purpose of the Plan is to maintain the standard of public services and the operation of the entity in accordance with the work program. |
| **Risk portfolio**  | Risk portfolio is the risk that groups records are present or may occur in one subject during operations.Grouping of risk will receive a risk portfolio that will be assigned to appropriate managers, and they will track your portfolio, overseeing the development and existence of an appropriate control environment and report (for example in relation to the area of ​​resources, or the legality and regularity). Thus grouped risks may relate to multiple goals. As an aid in grouping can be used "risk category". |
| **Business process**  | A set of related activities for the implementation of using funds of the budget and with the ultimate goal of meeting the needs and demands of the taxpayers for the services of appropriate quality in a given time period. |
| **Acting on****risks / addressing risks** | Responding to risk is considering possible measures that may affect the acceptability of risk. This could include risk avoidance, risk transfer, risk acceptance and tolerance of risk reduction or mitigation of risk by introducing control activities. |
| **Risk Monitoring** | Monitoring is part of risk management cycle where is cheked are suggested control activities effective and do they prevent or mitigate certain risk. |
| **Transfer of risk** | Activity whose purpose is transfer of risk impact to third parties or sharing risks with third party. An example of risk transfer is insurance policy in which the owner of the risk transfer risk impact to insurance company. |
| **Preventive controls**  | Designed to prevent the occurrence of ineffiency, mistakes or weaknesses. They cannot guarantee that control event won’t occur, but they reduce the possibility of its occurrence.Examples of preventive controls include separation of duties, procedures for authorisation and approval, control access to property etc.  |
| **Acceptance of risks** | Decision with which we accept cost of risk impact if it occurs in future.Accepting of current level of risk and subject prepares plans for unforseen circumstances or settlement of impacts that will occur in case of the risk.  |
| **Risk assessment** | Process which on systematic way carries out assessment and determination of impact and probability of events that may threaten goal achievement. |
| **Risk register** | Summary of identified and assessed risks based on impact and probability, activities needed and controls that will reduce consequences of risk and persons responsible for implementation of certain activities and deadlines for their implementation. It is an internal document of each subject. |
| **Risk** | Risk is possibility of occurrence of event that may adversely affect achievement of objectives and threat to achievement of objectives, programmes or services to citizens; risk can be seen in positive way as lost opportunities. Therefore, risk are all factors which may positively and negatively affect the goal achievement, and is characterized by the probability or possibility of occurrence of events and impact or consequence that will occur. Examples of risk in public sector:a) Uneconomical, inefficient or ineffective management of public fundsb) improper and illegal businessc) irresponsible business, irregularities and fraud with the consequence of loss of propertyd) unreliable reportinge) Inability to react on changing circumstances or inability of management in changing circumstances in a way that prevents or minimizes adverse effects on the provision of public services.f) everything that can harm the reputation of the subject and reduce public confidence |
| **Strategic goals** | Define the desired results and derive from mission of operations, and originate during strategic planning; as a rule they are multiannual and determine expected results. |
| **Strategic planning** | Management process by which the subject determines its direction of development and in line with that make decisions on the allocation of financial, material and human resources. As a result of a planning a strategic plan is adopted – document which consists of vision, strategic goals, ways of fulfilling goals (action plan), measures of assessment results and system of tracking of results achievement. |
| **Reducing or mitigating risk** | Taking actions and decisions in order to reduce probabilty of occurence or/and impact the risk. By threating risk is considered establishment of appropriate control activities in order to reduce probability of occurence of adverse effects associated with risk. |
| **Risk management** | Risk management is process of identification, assessment, monitoring and control of circumstances, which may adversely affect realization of established objectives of entity and taking necessary measures for reducing risks to to level of reasonable assurance that objectives will be achieved. It is an integral part of the planning and management of business processes. |
| **Risk identification** | The process of identifying events and determination of key risks which may affect achievement of organizational goals. |
| **Impact** | Quantative measure of the consequence of event.It usually presented as high, moderate or low. |
| **Effectiveness** | The maximum increase in output or outcome/ results of activities in respect of inputs; or the best ratio between results and funds used for their achievement. |
| **Vision** | Assumes perfect future; indicating long term direction and development. |
| **Probability** | A quantitative measure for possibility of risk occurrence.It is usually presented as low, medium or high probability. |
| **Person responsible for coordinating of establishment and implementation of risk management process at entity level.** | Encourages culture of risk management and assist managers in effective risk management, strengthening awareness of managers about risk management importance. |
| **PIFC Law** | This Law regulates the system of internal financial control in public sector of Montenegro including financial management and control and internal audit, determination of methodology and standards and other issues of importance for establishment, development and implementation of internal financial controls in public sector.Establishment and development of system of internal financial control in public sector in Montenegro is coordinated by Ministry of Finance. |