Republic of Macedonia
Ministry of Finance
Public Internal Financial Control Department

Risk Management Guidelines

Skopje, March 2015

PRELIMINARY REMARKS

The purpose of this document is to outline the overall approach to managing the risks facing public sector institutions, which will enable effective identification and management of their risks.

Risk management consists of two parts:

1. **Analysis of risk**, which involves the identification and definition of risks, plus the evaluation of impact and consequent action.

2. **Risk management**, which covers the activities involved in the planning, monitoring and controlling of actions that will address the problems and weaknesses identified, so as to improve the likelihood of the Institution in achieving its goals.

The risk analysis (or risk assessment) and risk management phases must be treated separately, to ensure that decisions are made objectively and based on all relevant information.

Risk analysis and risk management are interrelated and undertaken iteratively. The formal recording of information is an important element of risk analysis and risk management. The documentation provides the foundation that supports the overall management of risks.

Internal and external auditors provide varying degrees of assurance about the state of effectiveness of the risk management and control processes of the Institution. Both managers and auditors have an interest in using techniques and tools that sharpen the focus and expand the efforts to assess risk management and control processes that are in place and to identify ways to improve their effectiveness.

Objectives of the risk management

1. To develop a risk map which will identify and rank all significant risks facing the institution and to assist pro-active risk management.

2. To rank all risks in terms of likelihood of occurrence and expected impact.

3. To allocate clear roles, responsibilities and accountabilities for risk management

4. To enable the annual financial report to include a summary of the process applied to reviewing the effectiveness of the internal control system.

5. To raise awareness of the principles and benefits involved in the risk management process and to obtain staff commitment to the principles of risk control.

TABLE OF CONTENTS

INTRODUCTION

Risk Management guidelines is intended to provide practical and theoretically advice and recommendations to staff and management of the institutions on how to implement the principles and key elements of the risk management methodology.

The Risk Management guidelines present a relevant methodology for carrying out risk assessment within each activity of the institution. The risk management methodology is developed in order to cover issues from risk identification, as well as assessment of an impact and likelihood of occurrence of the risk event. Attention is paid to the matter that risk assessment can be successful only where it is followed by risk mitigation activities. In order to achieve that, the everyday work of all organizational units of the institution has to be integrated with activities that help to reinforce regular monitoring of identified risks and the application of suitable measures for risk mitigation.

Risk Management guidelines sets out principles, concepts, recommendations and guidance for the specific risk management approach. In risk management, risk managers assess in a systematic and structured way, the weaknesses of the system and suggest some possible improvements to enhance the possibility of successful accomplishment of their tasks.

The application of a structured methodology creates an opportunity for collecting results of the assessment of the different sectors involved in the structure of budgetary activities in the institution.The most significant risks derived from departments of the institution and determine actions for risk management.

3

2 - RISK MANAGEMENT – KEY PRINCIPLES

2.1.   Definition

Risk can be defined as "Any event or issue that could occur and adversely impact the achievement of the institution, political, strategic and operational objectives. Lost opportunities are also considered as risk".

Risk can also be defined as a possible threat, an event (or complex of events), activity (or complex of activities) or inactivity that may cause loss of assets or reputation and threaten successful fulfilment of tasks set to the institution.

Risk management is a central part of any organisation's strategic management. It is the process whereby organisations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities.

As a consequence, the essential meaning of risk management is to improve organisation performance via systematic identification, appraisal, management and control of projects and system risks and risk events and situations that can have adverse effects for achievements of the organisation objectives.

2.2. Risk management objectives in the institution

The goal of risk management activity is to bring the risks of the institution to an acceptable level by carrying out measures that would mitigate the likelihood of risk occurrence, impact of risk realisation or both at the same time. In order to do this, one must first acknowledge that risks are a natural part of everyday activities and cannot be avoided, but can only be managed.

That means that certain level of "risk acceptance" should be pondered for each particular case in analysis. Risk acceptance is a degree of risk that the management is willing to accept in the pursuit of its objectives. Analysis of risks with defined level of risk acceptance may provide reasonable assurance that the objectives of the institution will be achieved. However, even a well-designed and operated risk management cannot guarantee that all objectives will be fully achieved.

The resources are always limited and it makes no sense to talk about total risk elimination or total risk prevention, but only about risk mitigation to the level accepted by the management.

Risk assessment is the second component of the COSO model.

In accordance with the COSO definitions, the main objectives of risk management activity should be the following ones:

- To ensure functioning of the structure of the institution as a whole;
- To ensure the achievement of the objectives for each part of the institution on its particular level and in according to its functions;
- To protect State financial interests against fraud, waste, legal violations and errors;
- To protect the resources;
- To ensure the accuracy and timeliness of information and its availability to the persons/authorities concerned;
- To ensure that adequate operating procedures are in place to manage crisis situations.

In order to achieve the above-mentioned objectives, all departments of the institution have to understand and support the concept and methods of risk management process. This methodology needs to be developed and spread throughout the institution from the top management level till the operational staff. The risk management has to be implemented as a comprehensive, workable structure and set of practical tools for preventing risks which might negatively affect efficiency of the operations of the institution. This requires bringing together the practices of all relevant activities and the harmonisation of the results of risk identifi cation / assessment in order to manage them rationally, successfully, and cost effectively.

2.3. Risk management typology

The following general risk typology can be used for general risk classification by management and the internal audit unit of the institution, when relevant. Typology has three purposes:

- Creating a common language to facilitate communication in the domain of risk management;
- Providing a tool that can be used in the risk identification to help management make sure that all risk aspects and potential risks have been considered;
- Analysing, consolidating and reporting risks.

Eight categories of risks have been identified in the context of the institution's activities:

- **Strategic Risk**: these concern the long-term strategic objectives of the institution (ex: lack of monitoring policy/unclear strategies or objectives/unrealistic or overestimated objectives/absence of agreed objectives and performance targets...);

- **Operational Risk**: these concern the day-to-day issues that the organisation is confronted with, as its strives to deliver its strategic objectives (ex: no reliable IT system, complexity of rules, complex operation [when the operation is complicated and diverse with a large number of actors involved], lack of guidance, external information/data are not received in due time…);

- **Organisational Risk**: (ex: lack of identified substitute, insufficient supervision arrangement / insufficient or inappropriate delegation of tasks/ inappropriate segregation of duties…);

- **Compliance Risk**: these concern such issues as data protection, no effective regulation, lack of adequate legal instruments, contradictory operational procedures, complex rules increasing the risk of misinterpretation or error in their application, acceptance of non-eligible claims caused by unclear rules and regulations…;

- **Performance Risk**: (ex: no goal monitoring system);

- **Financial Risk**: these concern the effective management and control of the fi nances of the institution such as fraud or irregularity, and the effect of external factors such as foreign exchange rate;

- **Reputation Risk**: (ex: negative external assessment);

- **Other Risk**: unclassified.

Moreover, the categories of risks identified above can be crossed with the three types of theoretical risks as below:

- **Inherent risk**: the risk linked to the nature of the activities themselves (ex: lack of guidance, complexity of activities, lack of documentation, large number of actors involved in the procedure, lack of traceability of the activity…).

- **Control risk**: the risk that errors or irregularities in the activities or underlying transactions (tasks) are not prevented, detected and corrected by the internal control systems (internal control or internal audit). (Ex: lack of segregation of duties, lack of supervision, relative inexperience staff, inadequate staffi ng relative to workload, control strategy does not take suffi cient account of risks, or "misses" a key risk area…).

- **Residual risk**: the risk remaining after the controls put in place to mitigate the inherent risk.

3 - IMPLEMENTING RISK MANAGEMENT VIA THE SEVEN KEY STEPS

Risk Management is an ongoing process that includes the different activities like identifying, assessing, prioritising risks, implementation and review of mitigating or corrective actions as well as in advance planning and control. Conceptually, seven steps of the general risk management model are intended to provide a common risk management approach:

- **Step 1 - Describing business processes and activities in the Book of processes**
- **Step 2 - Identification of the objectives on activities**
- **Step 3 - Inherent risk assessment for each activity**
- **Step 4 - Internal control system assessment**
- **Step 5 - Selection of risk response for residual risks**
- **Step 6 - Implementation of risk response: action plan**
- **Step 7 - Monitoring and reporting**

3.1. STEP 1: Describing business processes and activities in the Book of processes

The preparing of a processes register (mapping) and the preparing of a book of processes ensures uniformity in the running of business processes, identifi cation of activities carried out, responsibilities for carrying out an activity as well as the deadline within which they should be executed. It should be coupled with an overview of controls identified within the process ensuring the achievement of the process objective.

Business processes are a set of interrelated actions directed towards the achievement of business objectives. The listing of processes is the primary objective of the risk assessment.

Mapping of processes includes listing and describing all business processes. Mapping of all business processes results in gaining an overall picture on the manner in which the institution achieves its business objectives. It gives an overall description of the organisation and its activities and shows whether or not there are weaknesses concerning the process defi nition. The Book of Processes gives an overview of interrelation between the processes as well as of the opportunities for possible improvements in the institution.

See Annex No 1: "Summary of the Ministry of finance Book of processes".

3.1.1 Flow charts and audit trails:

Each business process is represented by a **global flow chart** (overview of the business process as a whole). Flowcharting can provide a concise overview of the process and aids in identifying inadequacies by facilitating a clear understanding of how the process operates.

Then, within each process, the main activities are described in some **detailed flow charts** and identified in some related **audit trail.**

The audit trail is a management tool used for tracing a process, from start to end, and across the different actors involved in the running of the process or activity.

Additionally, the audit trail provides reconstituting all individual transactions and operations implemented in a particular process.

The design and preparation of audit trail is based on process analysis aiming at describing and charting flows of activities with clear identification of the operations that are executed, organisational departments involved in the activities along with other bodies (FINA, budget users,….), resources used and results obtained.

The audit trail provides management with a clear vision of:

- Process/ activities of the process/ tasks of the activities,
- Objectives of the process /activities/ tasks,
- Department staff concerned (who does what in the activity),
- Inputs used for each task and the expected outputs,
- Legal, fi nancial and other documents governing and supporting the activities under the processes and the database that support the activity.
- Filing rules at each step of the activity.

The audit trail is up-dated on a regular basis with a view to ensure it reflects the current state of affairs of the user of budget's processes.The information necessary for preparing or updating flow charts is usually obtained by interviewing personnel at each "assessable unit" about procedures followed, and by reviewing procedure manuals, existing fl ow charts and other system documentation. Sample documents are collected and each organizational unit involved.

Staff is questioned about their specific duties. Inquiries can be made concurrently with the performance of transaction reviews, particularly when fl ow charts are being updated.

- o The purpose of developing those items (fl ow charts and audit trails of the business processes) is to acquire a comprehensive view of the organisation and thus to identify all potential threats (risks) in the processes of the institution.

All flow charts and audit trails for all business processes should be compiled in the Book of processes.

3.2. STEP 2: Identification of activities objectives

Each departments involved in the goals of the institution has some specific role and objectives that need to be fulfi lled in order to guarantee sound financial management, and to give a fair view of the accounting.

The identified objectives of the activities must be in line with COSO aims:

- Guaranteeing the quality of financial records,
- Safeguarding assets,
- Ensuring compliance with the regulations
- Making the institution more effective.

The objective of each process is what one must achieve through the activities or actions of the process. The objectives of the processes are identified in the Book of processes and in the risk assessment form for each activity.

Furthermore, the risk management implies filling an assessment form with the activity identifi cation and the kind of activity concerned:

- **Monitoring** having an effective regulation, an efficient strategy planning….

- **Business**: preparing, executing, supervising budget activities and accounting operations in accordance with the regulation…
- **Support function activities**: using a reliable IT system and adequate human resources…

The activity goal has to be described in the Risk assessment Form according to the purpose of the activity that has been identified in the previous step (documentation of processes and activities). The methodology is "**one risk, one form**". Thus, the assessor must fi ll out as many forms as the number of risks he has listed in the activity. Then these forms would have the same "**activity's goal**" description for all the different risks.

The "**Process owner**" is the person responsible for carrying out the process (usually the Head of Department). Only one person can be a process owner. This person determines the manner in which the process is to be executed and is authorised to make changes to the process. The process owner is nominated in the audit trails and in the risk assessment form. It is recommended to put a job position here (function) rather than just the name of the person, to avoid changing data when the person responsible for the given process leaves of the Department. This requires a continuous updating of the book of processes.

See Annex N°2: "Risk assessment form template".

3.3. STEP 3: Inherent risk assessment for each activity

Every risk identification should be based on accurate knowledge of the processes and activities of the institution, and on the environment in which it operates.

At the beginning of risk identification it is necessary to standardise the knowledge concerning risk assessment of the risk managers / coordinators and staff of the institution responsible for filling risk assessment forms.

Risk assessment is about identifying and assessing issues or events that affect the activities of the institution and impact achievement of the defined objectives.

3.3.1 Identification of inherent risk:

Inherent risk may be defined as the potential for nonachievement of the organisation's mission, objectives and goals; waste, inefficiency or ineffectiveness; loss, unauthorised use or misappropriation of assets; non compliance with laws, regulations, policies, procedures and guidelines; or the inaccurate recording, preservation, and reporting of financial and other key data.

This analysis should be performed without regard to controls that are in place to counteract those risks.

The factors that to be considered in analysing the inherent risks are among the following:

- Purpose and characteristics of the activity;
- Budget and resource level;
- Procurement of goods or services;
- Impact outside of the institution.

Both managerial and operational staff should notify potential threats regarding their functions by submitting risk assessment forms to the Risk Manager / Coordinator of the institution for

approval. At this stage of the process, the person filing the risk assessment form should give a preliminary assessment of the risk, based on two indicators:

- The **likelihood** of the identified risks to occur (likelihood implies the frequency of an event's occurrence),
- **The impact of the risk**, i.e. the effect or consequences arising from the occurrence of the risk (impact implies consequences caused by the occurrence of an event).

The assessment process is an opinion based on the expertise and experience of the risk assessor and on the level of information available. The inherent risks are described in the Book of processes (main risk) and in the risk assessment forms of the activities, which are gathered in the risk mapping.

3.3.2. Risk impact assessment:

The impact assessment should be considered regarding financial stakes and foreseeable consequences on the process or institution.

Assessment	Interpretation
Minor	If the risk occurs, business process and planned activities are not disrupted (or are lightly impacted). Examples: Schedule delays to minor projects/services Loss of assets (low value) Unfavourable media attention
Moderate	If the risk occurs, the activities are significantly disrupted. Examples: Disruption of some essential programs/services Loss of assets Some loss of public trust Negative media attention
Severe	If the risk occurs, the activities are heavily disrupted. Examples: Disruption of all essential programs/services Loss of major assets Significant loss of public trust Public outcry for removal of Minister and/or departmental official

The assessor must determine the potential impact of the risk (**minor**/ **moderate**/ **severe**) and justify his/ her choice in the assessment form.

3.3.3. Risk impact assessment:

The likelihood is the posibility to occur any risk in analized working process.

Assessment	Interpretation
Low	The risk occurrence is unlikely or there is some knowledge of the occurred situation.
Medium	The event should occur sometimes. Previous evidence or knowledge of the occurred situation supports the likelihood of risk occurrence.
High	The event is expected to occur in most circumstances. Clear and frequent evidence or knowledge of the occurred situation supports the likelihood of risk occurrence.

For each risk, the assessor/coordinator must determine the level of risk likelihood (**low/ medium/ high**). The chosen level of the risk likelihood must be briefly justified in the assessment form.

It has to be taken into account that a risk identification should not be too general (so that no certain risk mitigation measures can be found) or too detailed (bringing out all possible risk situations, scenarios and risk mitigation measures would be too time-consuming and does not focus on the most important objectives of the institucion. Risk has to be identified and recognised as a realistic possibility by the majority of assessors.

The crossing between the risk likelihood assessment and the risk impact assessment is modelled in the **inherent risk matrix**:

Inherent Risk Matrix

Im pac t	*Severe*	Medium	High	High
	Moderate	Low	Medium	High
	Minor	Low	Low	Medium
		Low	*Medium*	*High*
		Likelihood		

See Annex N°3: "Model of Risk Mapping

3.4. STEP 4: Internal control system assessment

3.4.1. Criteria of control activities

Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the institution, at all levels and in all functions. They include a range of activities as diverse as approvals, authorisations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

In order to be effective, control activities must be:

- **Adequate** (right control in the right place and commensurate to the risk involved);
- **Cost-effective** (the costs of implementing a control should not exceed its benefits);
- **Comprehensive**, understandable and directly related to the control objectives;
- **Consistent** with their operation in line with the Internal Control plan for a certain period.

3.4.2. Categories of internal control activities:

Types of controls can be categorized as follows:

- **Directive control activities** are designed to guide an institution toward its desired outcome. Most directive control activities take the form of laws, regulations, guidelines, policies and written procedures.
- **Preventive control activities** are designed to prevent the occurrence of an undesirable event. The development of these controls involves predicting potential problems before they occur and implementing ways to avoid them.
- **Detective control activities** are designed to identify undesirable events that do occur, and alert management about what has happened. This enables management to take corrective action promptly.
- **Corrective control activities** are processes that keep the focus on undesirable conditions until they are corrected. They may also help in setting up procedures to prevent recurrence of the undesirable situation.

There is no one-control activity that provides all of the answers to risk management problems. In some situations, a combination of control activities should be used, and in others, one control activity could substitute for another.

The concepts of directive, preventive, detective and corrective controls, as well as the control activities described above, apply to both manual and computerized processes.

3.4.3. Assessment of the existing / established and expected / needed controls within business processes:

Control activities mitigate processing risks. Control activities are the policies and procedures that help ensure that management directive are carried out. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliation, reviews of operating performance, security of assets and segregation of duties.

The different categories of Control Activities are classified in 8 points or factors grouped in 3 main issues: **organisational issues, documentation issues**, and **traceability issues** as regards each institution`s activity.

Main Issues of control level	Factors
1. Organisational issues	1.1. The organisation (Who does What?) 1.2. The different level and steps of control 1.3. Assets and document that support general arrangements
2. Documentation issues	2.1. Existing Documentation 2.2. Compliance with existing documentation
3. Traceability issues	3.1. Players identification 3.2. Transactions traceability 3.3. Controls traceability

This analysis is performed with Internal Control questionnaire (around 30 key questions relating to the 3 main issues mentioned above). The methodology that use is "one risk, one questionnaire", and the answers to this latter are supported and corroborated with collection of documents, evidences.

The evaluation of the level of Internal Control system implemented is rank in four-category:

- **No control in place**: means that any kind of control does not exist at all. Therefore, the possible occurrence of the risk in very high.
- **Low**: means that controls exist but are not sufficient (ex: not relevant or not appropriate).
- **Medium**: means that the controls are relevant but are not able to cover the whole field of possible risk.
- **High**: means that the controls in place are relevant and operate effectively.

These indicators must be crossed with inherent risk level to obtain the control risk matrix. The scheme below identifies all the different possible combinations.

Control Risk Matrix					
I n h e r e n t R i s k L e v e l	*High*	*Low*	*Medium*	*High*	*High*
	Medium	*Low*	*Medium*	*High*	*High*
	Low	*Low*	*Medium*	*Medium*	*High*
		High	*Medium*	*Low*	*No control in place*
		Level of internal Control System Implemented			

See Annex n° 4: "Internal Control assessment questionnaire".

Evaluations of each activity's Internal Control System Implemented level are reported in a consolidated Excel sheet with final ranking combining both colour code and scoring (scale from 0 to 3):

- No Internal Control System in place (0 – Red)

- A low Internal Control System in place (1 - Red)

- A medium Internal Control System in place (2 - Amber)

- A high Internal Control System in place (3 - Green)

- Not applicable (Neutral - Black)

	Level of Internal Control System Implemented	BP01	BP02	BP03	BP04	BP05	BP06	BE01	BE02	BE03	PDM01	PDM02	PDM03	PDM04	PDM05	BS01	BS02	BS03	BS04	ASFR01	ASFR02	GLOBAL
3	1.1. Organisational issues																					
4	1.1.The organisation (Who does What?)	00	0,50	0,57	0,50	0,50	0,50	0,50	0,0	0,57	0,0	0,62	0,57	0,0	0,0	0,56	0,0	0,56	0,56	0,0	0,43	0,53
5	1.1.1.The institution put in place job descriptoins describing for each job, both, functions, tasks and duties, and related candidate profile expected ?	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	
6	1.1.2. The institution put in place annual or multi-year written mission letters prescribing Specific Measurable Achievable Realistic and Timely (SMART) goals to achieve (Departmen level) ?	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
7	1.1.3. The institution put in place annual or multi-year performance indicators ?	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
8	1.1.4. The institution is described in a organisational chart regularly updated and mentionning necessary functions, incumbent, substitute, delegations, IT systems authorisation, bookkeeping and related accounts authorised...?	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
9	1.1.5. The institution follows and updates the IT systems and database (Excel) list used by Sector, Users and Activities ?		2	2	2	2	2	2	2	2	3	3	2	2	2	200 %	2	2	2	2	2	
10	1.1.6. Delegation of authority limits are clearly defined, assigned and communicated in writing ?	1	1	1	1	1	1	1	1	1	1	1	1	1	1					1	1	
11	1.1.7. The organisational chart includes segregation of tasks for incompatible functions?	2		3						3	3	3	3	3	3	2	2	2	2	1	1	
12	1.2 The diferent level and steps of control	0,0	0,73	0,67	0,67	1,00	0,83	0,81	0,0	0,71	0,0	0,67	0,70	0,0	0,0	0,0	0,0	0,73	0,0	0,0	0,46	0,68
13	1.2.1. Computerised control system is integrated within IT systems that is used?			2	2			3		3		3		1						2	2	
14	1.2.2. For some transactions on ex-ante control procedure is obligatory?			2	2	3		3		3	2	2	3		2		2			2	2	

The main goal for each activity of the institution is to identify activities concerned, both at operational and managerial level:

- The main strengths and weaknesses
- The area (s) where Internal Control System must be improved.

For each one of the 8 measurement factors, a scoring is automatically done, from 0 (low) to 1 (high) and a graphic representation is generated around these 8 points of controls. This tool can be used indifferently by activity, by issue or for all activities of the institution.

3.5. STEP 5: Selection for risk response for residual risks

Residual risk can be defined as being the risk remaining after the controls put in place in order to mitigate the inherent risk, and can be summarised as follows:

Residual risk = Gross inherent risk – risk mitigated by control procedures.

The 'residual risk' is that remaining once these measures are taken. Residual risk is deduced from inherent risk and control risk. The scheme below gives the risk matrix.

Residual Risk Matrix

Inherent Risk				
	Severe	Medium	High	High
	Moderate	Low	Medium	High
	Minor	Low	Low	Medium
		Low	*Medium*	*High*
		Control risk		

3.6. STEP 6: Implementation of risk response: action plan

The risk managers and the risk manager co-ordinator must prepare an action plan. There are several possible strategies for mitigating risks and all of these strategies can be used and the risk manager should determine how to manage them. The decision will depend on the significance of the risk and management's risk tolerance and risk attitude (certain risks may be accepted, other not or just to a limited degree). In principle there are four (4) main strategies to use as a risk response:

- **Avoid** - Actions are taken to discontinue or modify the activities/objectives giving rise to risk. Risks can be avoided by changing the scope of the activities, even by changing the regulation;

- **Transfer** - Actions are taken to reduce risk likelihood or impact by transferring or sharing a portion of the risk with third parts. Risks can be reassigned to third partners that best able to control them or (if it is different) who will carry the risk at lowest level;

- **Reduce** - This is the most common risk response. Actions are taken to reduce the risk likelihood or impact or both. This can be done in various ways, for example enhancing legislation, simplifying operational procedures, increasing control of staff or obtain more information through feasibility studies or specific research;

- **Accept** - No action is taken to further reduce the risk. Risk manager estimates that perceived risk level can or has to be accepted or thinks that the cost of reducing the risk is higher than the potential damage.

The impact of the risk may be tolerable without any further action being taken. Even it is not tolerable, the institution might be not able to do something to mitigate the risk, or the cost of taking any action might exceed the potential benefits gained. Risk managers must justify his choice, in particular in the case where no action is undertaken (tolerance analysis).

3.6.1. Determination of acceptable risk level:

The 'residual risk' level (i.e. the risk level taking into account existing controls and mitigating actions) depends on risk level and management's risk acceptance or tolerance. Management decides if additional measures are needed to further reduce residual risk level or has to be accepted. In some cases, residual risks may have to be accepted for several reasons. Firstly, reducing the risk exposure to «zero» would demand very significant control measures whose costs would be disproportionate to the benefits. Secondly, certain risks are outside of management control.

In managing risks, the assessor or risk manager should focus both on the internal factors of the organisation (such as the quality and motivation of the staff, turnover of staff, quality of control systems or rapid growth of workload, etc.) and external factors (such as the existing legal environment and the possibility of changes in legislation, technological developments, the general risk environment in which the institution is operating, ….)

In general, a risk with a low impact and a low likelihood of occurrence does not need any further consideration, whereas a risk with a high impact and high likelihood will require priority action. However, there could be situations where the management estimates that the risk can or has to be accepted even thought it is critical. This is typically the case when management does not control the risk (external risks).

The management decides which risks belong to a low level of acceptance and if additional mitigation activities are not necessary or not. The risk manager may decide that in some activities, high risks are accepted.

On the other hand, the risk manager can decide that mitigation activities need to be carried out in the case of medium or low risk level.

3.6.2. Implementation of risk response:

Implementation of the risk response means to adopt the appropriate measures in order to minimize the likelihood and impact of the risk event in direction to zero. Appropriate measures implementation requires however to make a clear distinction between consequences of the event or risk occurring/ risk symptoms and the causes of the event/ risk occur.

A bow tie diagram can easily support this approach by defining:

- the event or event to be prevented
- threats that could cause the event to occur
- consequences of the event occurring
- controls to prevent the event occurring and
- controls to mitigate against the consequences.

1st step:
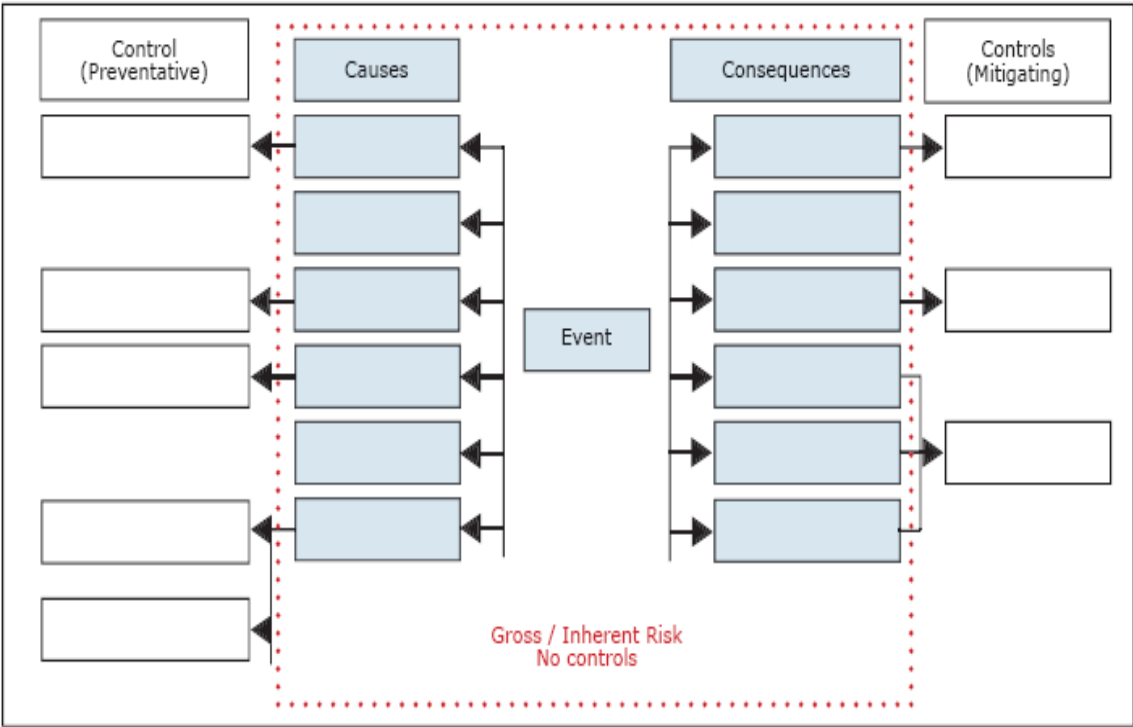
2nd step:
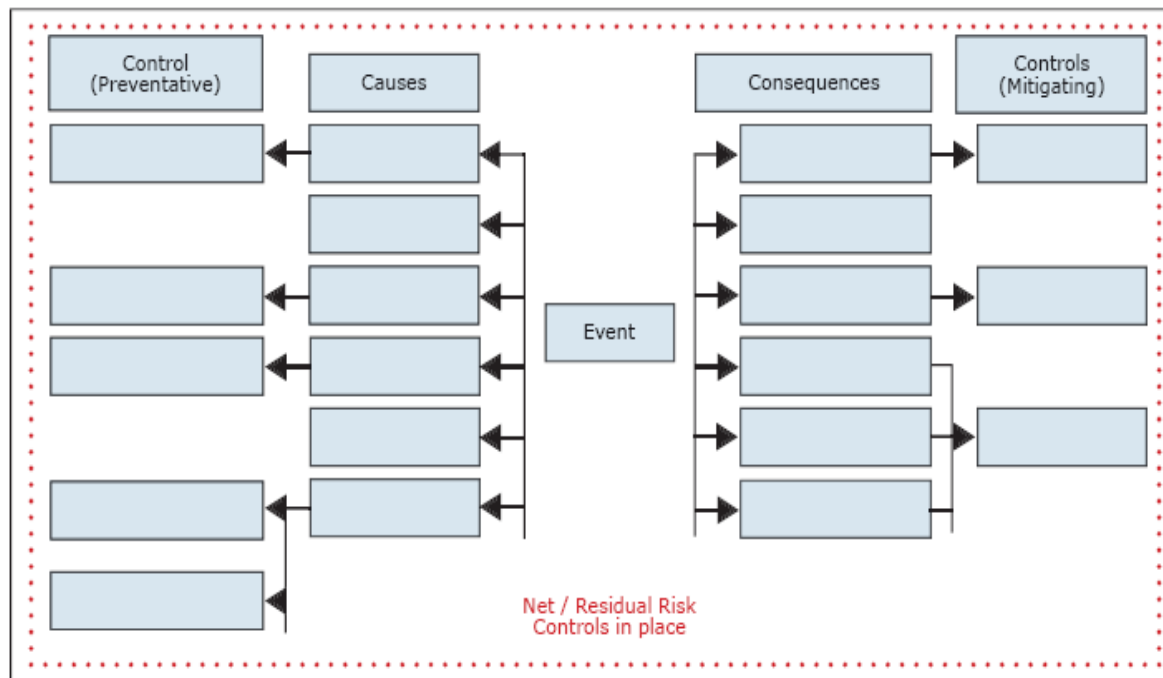
Appropriate action plan, corresponding to the selected risk responses, should be established to ensure that concrete measures are taken to reduce the risks (causes of the risks).
In some cases when the risk can be reduced immediately or within a short period of time, no elaborated action plan is needed. The management of other risks may require substantial efforts over a long period of time (e.g. modified legislation, new IT systems, changing organisation and management structures, etc).

That is why the action plan need to content folowing information:

- A detailed description of the risk;

- A detailed description of the actions / measures to be taken;

- The person responsible for the actions / measures to be taken;

- Target deadline for each phase of the project, and the final target deadline;

- Resources needed to implement the plan (if necessary);

- Expected results of the action.

Control risk corresponds to the risk that a misstatement or an error that could occur in implementing activity and will not be prevented or detected and corrected on a timely basis by the internal control systems.

The 'control risk' is limited by ensuring an effective programme of checks is in place, designed to verify the legality and regularity of the transactions.

Examples of control risk indicators: staffing/ workload levels, staff turn over level, number of complaints/claims, fi gures of errors automatically or manually detected by internal control system, figures of errors detected by other control instances/levels (higher level within the control systems, Supreme Audit Institution).

3.6.3. Implementation of control:

The article 16 of the PIFC Law currently regulates the control. The control must take into account the three following findings:

A)Internal control measures:

- **Preventive actions** are designed to prevent the occurrence of failures, inefficiencies, errors and weaknesses. For that reason, preventive controls are proactive measures operating during the course of an activity. These controls constitute the best practice in terms of their cost, as they prevent losses and reduce certain risks. They must assess through four criteria: monitoring; organisation; documentation; traceability.

Ex: segregation of duties, authorisation and approval, assets for access control, checking arithmetical accuracy before payment.

See Annex No 5: "Model of Organisational / Functional Chart".

- **Detective actions** are designed to detect and correct failures, inefficiencies, errors and weaknesses. They operate after an event has occurred and they should reduce remedial activities. Detective controls are used to improve procedures or preventive controls. They must be implemented by filling out the "Internal control sheet". If not, the internal control system is considered not to be relevant or reliable.

  Ex: reconciliation between the payment order and the receipt.

- **Corrective measures** are designed to correct the circumstances arising from the undesired events that came true. They must be traced by detected errors documents or files.

See Annex No 6: "Models of control sheet".

In practice, the above categories may not be clearly distinguished and a single control may operate to cover two or more functions. For instance, supervision covers preventive and detective controls.

B) Management of the level of control :

Segregation of duties		**Stakes/ Impact**	High	Segregation of duties Preventive or Ex ante controls
Low				High
Segregation of duties not necessary Low level of control				**Risk/ Occurence**
			Low	Segregation of duties Ex post controls
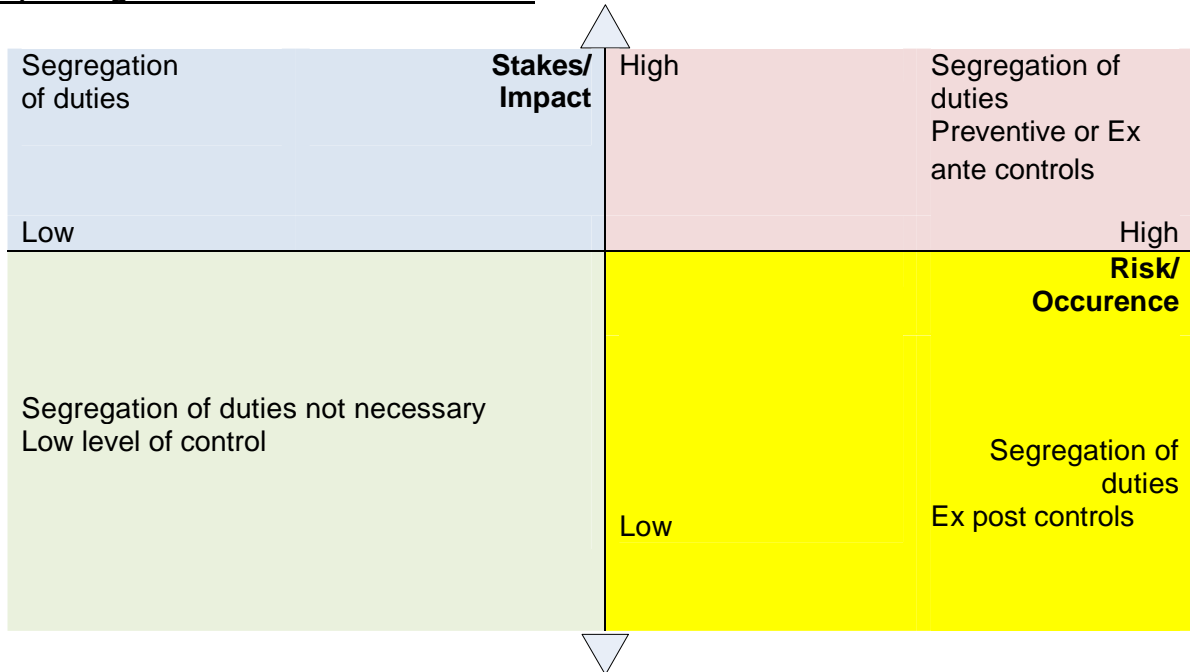
The level of control must be adjusted both to the risk impact and to the risk occurrence. It must be periodically considered by the Management.

C) Internal Control Monitoring:

Internal control systems need to be monitored – a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing or separate evaluations are designed to provide information on whether internal control over financial reporting remains effective. Monitoring facilitates timely identification of control failures and remediation.

On-going evaluations are designed to provide continuous monitoring of the controls. Separate evaluations (internal audit) need to be carried out by knowledgeable personnel with suffi cient frequency and scope to manage the risks associated with control failures. Internal control deficiencies should be reported upstream, and serious matters reported to top management.

Monitoring is effective when it is designed such that control failures or deficiencies are identified in a timely fashion, communicated to those who have responsibility for the controls, and the correction of the control deficiency in a timely fashion is facilitated.

3.7. STEP 7: Monitoring and reporting

Risk exposure changes over time. Risk responses that were once adequate may become irrelevant; control activities may become less effective or no longer performed. For instance, new risks may emerge during the year as a result of:

- modifications in activities and objectives,
- re-organisation of management structures or systems and
- changes in external working environment.

New risks can be determined by:

- regular management activities,
- internal control,
- ex-ante / ex-post controls and
- other verifications and analysis.

In order to ensure that the action plans of the institution continue to be relevant and effective at all levels, regular monitoring and reporting should be carried out. Since already identified risks may evolve and new risk may emerge, monitoring is also needed to ensure that risk register is kept up-to-date.

The Risk register includes the risk mapping and the action plan follow-up.

3.7.1. Risk Mapping:

Risk mapping is a tool used for the identification, control, and management of risk.

By considering the risk mapping approach the institution should be aware it is not a one shot solution and the results are not carved in stone. Rather it is an iterative process that refines management understanding of the exposures that it is managing, and measures the effectiveness of staff in mitigation of the controlling risk.

The risk mapping process includes the six following steps:

- **Identify**: risks must be identified in order to ensure that the full range of significant risk is encompassed within the risk management process. The final 'risk map' should be checked for consistency with the strategic and operational plan of the institution and intended risk management processes.
- **Understand**: existing risk measurement and control processes should be documented.
- **Evaluate**: this involves estimating the frequency of loss events, estimating potential severity of loss events, and considering offsetting factors to limit frequency or severity of losses and understand potential control processes.
- **Prioritise** the evaluation of risk frequency, severity, and controls form Step 3 are then consolidated. The risks are ranked according to a combined score incorporating all three assessments. The ranking starts with the risk with the worst combination of frequency, severity and control scores.

- **Manage**: the consolidated evaluations from Step 4 should then automatically indicate the risks that need the most attention. The critical stage involves deciding how to manage the most important and largest risks, considering with the institution`s strategy and objectives.
- **Revisit**: the process of identifying, understanding, evaluating, and prioritising risks must be repeated regularly in order to ensure that the key risks are being appropriately managed.

Each year or ideally half-year, management will review what happened in the recent past and assess whether risk management efforts produced the expected results. Then it is ready to start the process again from Step 1.

The **risk mapping** architecture reproduces:
- into the columns the structure used in the assessment forms;
- into the lines the division into processes and activities.

The three risk levels can be spotted immediately on the risk-mapping table by the three different chosen colours:

- green for "low";
- orange for "medium";
- red for "high"."

This colour typology is identical as the one used in the risk assessment form.

The Risk mapping is mainly filled out with all the forms approved by the risk managers (their role is explained more in detailed in chapter 4.2.2). However the Risk Management Coordinator (his/her role is explained more in detailed in chapter 4.2.3) must take into account the conclusions or recommendations coming from the external and internal audit reports to adjust the different risk levels (inherent risks; control risks; residual risks).

Only the RMC is in charge of the last column "**central risk level**". From the assessment level carried out by the Risks Managers, the RMC must rank the risk mitigation priorities. The prioritisation must be based on the financial stakes of the activities and on the strategic goals decided by the top management (State Secretary level).

3.7.2. The Action Plan of the institution:

The plan should contain activities necessary for the implementation of the financial management and control system, deadlines for execution, and persons responsible by individual activities. The Risk Manager Co-ordinator holds the consolidated action plan.

See annex No 7: "Model of Action Plan for weaknesses elimination".

3.7.3. General scheme: Risk register feeding

According to this scheme, the Risk Manager Co-ordinator is responsible for the final treatment of the information concerning the risks detected in the institution.

In order to prioritise the internal control actions, he has to reconcile the different information inputs (risk assessment forms, internal and external audit conclusions) and possibly manage the contradictions that could emerge from these confrontations of information.

4. RISK MANAGEMENT STRUCTURE AND RESPONSIBILITIES

4.1. Risk Management strategy

Risk identification and assessment involve the preparation of the risk management strategy, approved at the highest management level.According to article 15 of the Public Internal Financial Control Law - PIFC, (Macedonian Official Gazette № 90/09 and 188/13), each entity has an obligation to prepare a risk management strategy. Control activities concentrated on risk reduction must be analysed and updated at least once a year.

Regarding the development and functioning of management and control system in the institution, it is important that all those involved in the institution's processes have an overall understanding of the risk management used as a management tool.

The overall risk management will derive from the risk measurement and prioritisation. The purpose of managing risks is to constrain them to a tolerable level. Any action that is taken by the institution with a view to manage a risk becomes part of the "internal control".

The identification of risk factors presumes good cooperation between all organizational units and all management levels of the institution. In designing control it is important to give reasonable assurance that the associate risk will be constrained rather than eliminated. Every control action has an associated costs. Hence it is important that the control action offers value for money in relation to the risk it is controlled.

4.2. Risk Management structure of the institution

Implemented risk management activities should effectively follow functional relations between departments involved in the processes of the institution.

Therefore, in order to effectively implement and conduct risk management activity, the functional responsibilities have to be defined within risk management structure. It includes:

- Each staff member or official of the Institution;
- Risk Managers (RM) from every Department;
- The Risk Management Co-ordinator (RMC).

Architecture of the internal control system
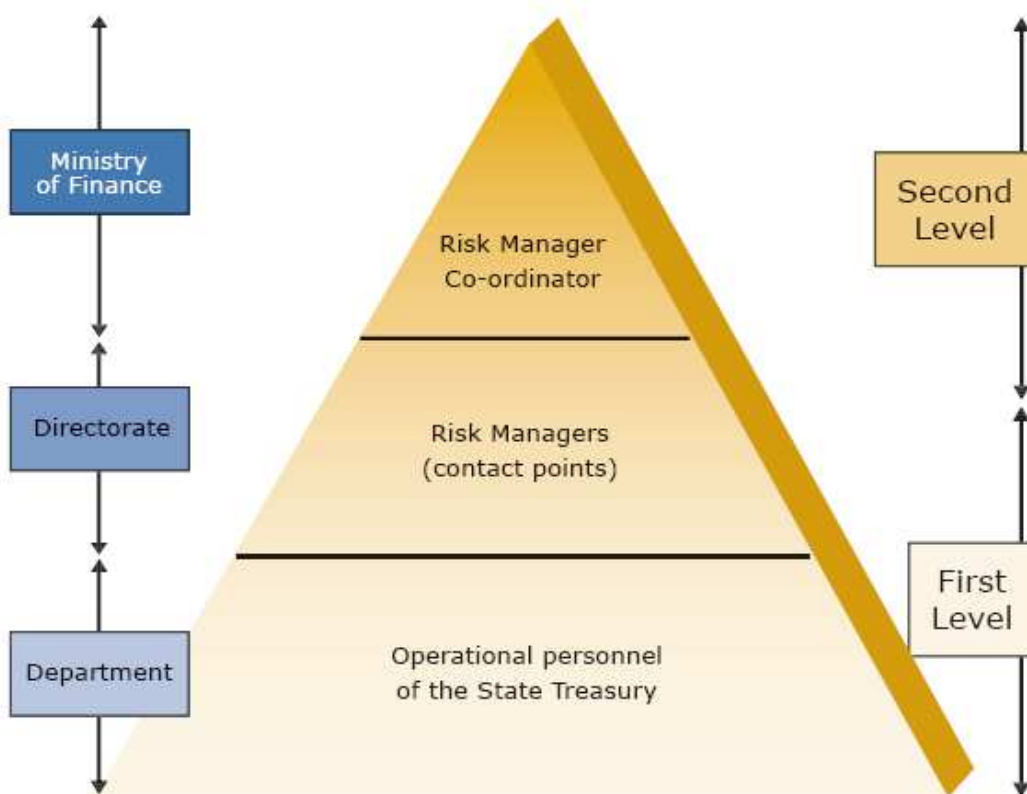
The diagram shows the two levels of internal control in the Macedonian Ministry of Finance.

Risk manager should be appointed in each department in the institution. His role is to verify the level and type of identified risks by the operating staff or management.

See Annexes No 8: "Organisational flow chart for the risk management" and No 9: "First and second level of control activities".

4.2.1. Staff of the Institution:

It is the main part of the first level of internal control system in a bottom-up approach based on a declarative assessment. Indeed the methodology is based on self-assessment, from the the state of internal control and the risk assessment form.

The Staff of each Department in the institution must fill the Risk assessment Form twice a year (regular updating).

See annex N°2: "Risk assessment form template".

4.2.2. Risk Manager (RM):

The Risk Managers are responsible for risk management in each Department of the institution. The duties of the Risk Manager are to:

- collect the risk assessment forms and ensure that they are completed correctly,
- supervise the risk level and risk justifications of the assessment forms (formal approval),
- forward the risk assessment form to the Risk Manager Co-ordinator;
- follow the action plans coming from the different departments of the institution,
- ensure that there is a culture of risk awareness in the institution.

Risk Managers should be aware that Risk assessment forms are normally filled without taking into account the existing mitigation measures, e.g. by internal control measures.

4.2.3. Risk Management Co-ordinator (RMC):

The Risk Management Co-ordinator is responsible for the risk assessment of the operating structure in the institution. He has to collect and compile risk assessment forms from all Risk Managers. In addition, the RMCs must be aware of the high risk identified and should take action to ensure communication of risks identify. RMC should also ensure a continuous risk assessment, monitoring of risk levels, in order to determine trends of occurrence (update of the risk registers).

Depending on the nature of the risk and scope of his responsibilities RMC could undertake necessary actions regarding risks inside his competency.

The duties of the RMC include:

- collecting the risk assessment forms received from the various Risk Managers;
- evidence of the details from the risk assessment forms in the Risk Register (risk mapping) and consolidated action plan;
- reviewing the risk assessment forms and collection of further information if needed;
- monitoring the progress of risk mitigation;
- elaborating of the mapped risks and its half-year updating.
- consolidating action plans for the whole institution and following their implementation.

It is the responsibility of the RMC to ensure that the Risk Managers are trained in and actively support the risk management process.

Risk mapping should be available to all staff of the institution, in order to give risk assessment added value and enable more efficient solutions of the differences concerning offered mitigation activities, deadlines and responsible persons, adding mitigation activities and consolidating similar risks that are determined by different organizational units.

After receiving a risk assessment form from the Risk Manager, the RMC should ponder if the risk is already covered by internal control measures, and to what extent. Additionally, the

conclusions and recommendations given by internal auditors and laid down in internal audit reports should also be considered by the RMC when updating the risk mapping.

Organisation of risk managers meetings on a regular basis is recommended. The RMC should set up the agenda of these meetings.

5 - FOLLOW UP AND ANNUAL REPORTING

5.1. Follow up: annual review and risk register updating

The RMC must conduct an annual review of its internal control activities as a basis for the statement on internal control in the annual report.

Every year the RMC must update the risk register and re-evaluate the risk level of the "central risk level" in the dedicated column of the risk register. In addition, the Coordinator shall prepare a report which will be taken into account in preparation of the annual report on the internal control system in accordance with Article 47 of the Public Internal Financial Control Law.

5.2. Annual report

Current situation:

The report is prepared annually and only on the basis of internal control self-assessment questionnaire and the Manual for FMC. The structure of this annual report includes all 5 components of internal control system (control environment, risk management, controls, information and communication, and monitoring).

Improvement proposals:

The annual report to be made by the institution is strategically important document that provide everincreasing of quality standards for managerial accountability.

The purpose of this report is to measure progress made annually in the institution. Logically, this report should provide an annual summary evidence of the institution's activities in the field of financial management and control and include an assessment of the institution's efforts to approximate its financial management and controls system up to the EU best practice.

The report should be as much as possible **operational and problem solving oriented** and should should provide recommended actions for further improvement.

In terms of content, annual report must make reference to **the improvements** and **developments** achieved in the relevant period compared to the situation in previous years. The improvements, though, relate especially to the legislative and methodological developments, training and institutional capacity of FMC and risk management.

It should also be mentioned that the State Audit Office and internal audit should make annual reports to assess the quality of financial management and control (audit opinion on internal control system). State Audit Office started with performance audits of the financial management and control system and internal audit to provide external assessment of the PIFC system.

This internal control report of the institution must include the following parts:

- Reference frameworks and initiatives contained in the report.
- The environment of the institution's internal control system:
  - The institutional environment;
  - The objectives, methods and scope.
- Participants in the risk control system:
  - Internal control supervision participants (Risk Managers, Cordinator);
  - Operational organisation of risk control;
  - Periodic evaluation of the internal control system by the audit function (internal and external audit).
- Internal control strategy: an overall risk control system in order to achieve an ongoing improvement
  - Management steps of the internal control system risk register: risk mapping and action plan
  - Organisation of the departments, ongoing adjustments of controls to risks
  - Documentation of the working processes of the institution, activities and risks
  - Traceability of participants: strengthening the audit trail
- A maturity level assessment of fiscal risk management.
- Conclusion and outlook.

See Annex No 10: "Template structure suggested for the Annual Report".

ANNEXES

- **Annex No 1: "Summary of the Book of processes"**

- **Annex No 2: "Risk assessment form template"**

- **Annex No 3: "Model of Risk Mapping"**

- **Annex No 4: "Internal Control Assessment Questionnaire"**

- **Annex No 5: "Model of Organisational / Functional Chart"**

- **Annex No 6: "Models of Control Sheet"**

- **Annex No 7: "Model of Action Plan for weaknesses elimination"**

- **Annex No 8: "Organisational flow chart for the risk management"**

- **Annex No 9: "First and second level of control activities"**

- **Annex No 10: "Template structure suggested for the Annual Report"**

LIST OF THE BUSINESS PROCESSES OF MINISTRY OF FINANCE

1. BUDGET PREPARATION

1.1 Fiscal impact assessment of legislation and international agreements and treaties

1.2 Developing instructions for the preparation of the Budget proposal for the tree year period

1.3 Preparing and drafting the Budget and its consolidation

1.4 Drafting and approving the reallocation of the Budget funds to 20% and to 10% for salaries and allowances and a decision on the reallocation / rebalance of budget funds (over 20 %)

1.5 Drafting Government Decree on the manner of calculating the amount of equalization for the decentralized functions of local government

1.6 Financial aids from State to Local Self- governments

2. BUDGET EXECUTION

2.1 Payment execution in accordance with adopted Budget and other normative acts

2.2 Liquidity planning and financial flow of the Budget Management

2.3 Foreign currency payment operations

3. PUBLIC DEBT MANAGEMENT

3.1 Developing a strategy and annual plan of borrowing

3.2 Borrowing funds at the domestic market through issuing bonds

3.3 Repayment of matured liabilities

3.4 Collection of activated State Guarantees

3.5 Issuance of Government Guarantees

4. BUDGETARY SUPERVISION

4.1 Working in the office on received petitions/request

4.2 Preparation for / Budgetary Control

4.3 Execution of inspection / Direct Budgetary Control

4.4 Taking inspection measures for Budgetary Control

5. ACCOUNTING AND STATE FINANCIAL REPORTS (State annual account)

5.1 Bookkeeping expenditure and revenue

5.2 Consolidated Financial State statements (annual accounts)

5.3 Rebooking (continous)

RISK ASSESSMENT FORM

	RISK MAPPING OF THE INSTITUTION	Risk Mapping Scale Reference
	Risk Mapping Scale	
Name, surname and function of the author		Date of the analysis
Name of the Cordinator / Risk manager		
Name of Process in wich risks are identificated		
Activity in wich risks are identificated		
Kind of activity	Monitoring / Controls	
	Business	
	Support / Service	
Name, surname and function of Process Owner		
Activity's Goal		
Kind of Risk having an impact on the achievement of the goal	Strategic	
	Operational	
	Organizational	
	Compliance	
	Performance	
	Financial	
	Reputation	
	Other (...)	
Risk identification		
Risk's Likellhood	Low	
	Medium	
	High	
Justification of the Risk's Likellhood		
Risk's Potential Impact	Minor	
	Moderate	
	Severe	
Justification of the Risk's Potential Impact		
Level of implementation on internal control system	No control in place	
	Low	

	Medium	
	High	
Justification of the Level of Internal control System Implemented		
Date of scale validation		

Signature of the Coordinator/Risk Manager   **Signature of the author**

_____   _____

Risk Inedtificating / Mapping
An example of identified risks (eg. Ministry of Finance)

Risk Mapping Scale Reference	Process Indentification	Activity identification	Kind of activity	Process Owner (Responsible Entity)	Activity Goal	Kind of Risk having an impact on golal achievement	Risk Identification	Risk`s likelihood	Justification of the risk Likelihood	Risk`s Potential Impact	Financial Impact (If applicable)	Justification of the Risk`s Potential Impact	Inherent Risk Level	Level of Internal Control System Implemented	Justification of the Level of Internal Control System Implemented	Control Risk Level	Residual Risk Level
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2009-BP 01a	Budget Preparation	1.1 Fiscal Impact assessment of legislation and international treaties and agreements	Business	Petre Petrevski	Check the assessment of the fiscal implications of the implementation of regulations and international agreements and contracts by direct budget users (expenditures and revenues) and opinion within a fixed period	operational	Not to be an expert in different areas to recognize the assessment made by direct budget users	Medium	It happens sometimes	Medium		The impact of the budget user depends on the amount	Medium	Medium	Communication with the departments concerned in case of difficulty and also Legal Affairs Sektor. It will be useful to have a dedicated person with knowledge of the law	Medium	Medium
2009-BP-01B	Budget Preparation	1.1 Fiscal Impactassessmentof legislation and legislation and international treaties and agreements	Business	Petre Petrevski	Check the assessment of the fiscal implications of the implementation of regulations and international agreements and contracts by direct budget users (expenditures and revenues) and opinion within a fixed period	organizational	Not enough knowledged staffto do the job due time (more than 300 documents from the beginning of the activity)	Medium	It happens between sometimes to very often	Medium		The opinion isnt given in time	Medium	No control in place	They do not give an advice if you do not have time. No action plan. There is only one solution, employing a further 2 persons, the head knows this need	High	High
2009-BP-02a	Budget Preparation Process and Local AuthoritiesBudget	1.2 Developing instuctions for the preparation of the State Budget Proposal for the three year period	Monitoring	Petre Petrevski	To develop Instuction adopted by Government (macroeconomic and fiscal projections , limits for all levels of government)	operational	Not to be able to respectthe deadlines	Medium	The likelihood is moderate. The previous budget calendar deadlines are overtaken but the 15th of November is strictly respected.	Low		The impact is minor, because if a delay in adoption of guidelines occures, a shorter deadline is given to budget users	Low	No control in place	Nothing can be done, it all depends on politics. Moreover, the medium-term strategic planning systems will have an impact on the respect of the deadline this year	High	Medium
2009-BP-02b	Budget Preparation Process and Local AuthoritiesBudget	1.2 Developing instuctions for the preparation of the State Budget Proposal for the three year period	Monitoring	Petre Petrevski	To develop Instuction adopted by Government (macroeconomic and fiscal projections , limits for all levels of government)	operational	Mistake in the determination of budget forecasting - forecasts (it is difficult to forecast wages and some subsidies)	High	No capacity to evaluate with accuracy the amount of wages (without a reliable IT system). Social and political issues relating to subsidies (railways, etc.).	Medium		Using re-allocation of funds when the risk occurred in the past	High	Low	Currently, there is poor control. In the future, it will have a high control over IT system.	High	High

INTERNAL CONTROL ASSESSMENT QUESTIONNAIRE

Internal Control Questionnaire Reference	

Name of person(s) in charge of internal control assessment:	

Date of the analysis:	

Process Identification:	
Activity Identification:	
Process Owner (Responsible Entity):	

Points of control	Reference documentation (for information)	Answer	Comments	Tools of control used (check list, control fiche, supporting documentation...) taking into account the requested controls	Test of controls sample corroboration result (if used)	Level of Internal Control System Implemented	Category of control (for information)
1. Organisational issues							
11.1. The organization (who does what?)							
1.1.1. The Ministry of finance put in place job descriptions describing for each job both functions, tasks and duties, and related candidate profile expected?	Organisational Chart, Book of processes						Preventive Directive

Question	Evidence						Type
1.1.2. The Ministry of Finance put in place annual or multiyear written mission letters prescribing Specific Measurable Achievable Realistic and Timely (SMART) goals to achieve (Director level)?							Directive
1.1.3. The Ministry of finance put in place annual or multi-year performance indicators?							Directive
1.1.4. The Ministry of finance organisation is described in a organisational chart regularly updated, and mentioning if necessary functions, incumbent, substitute, delegations, IT systems authorisations, bookkeeping and related accounts authorised…?	Detailed Organisational Chart, audit trail						Preventive Detective
1.1.5. The Ministry of finance follows and updates the IT systems and database (Excel) lists used?							Preventive Detective
1.1.6. Delegation responsibilities and authority limits are clearly defined, assigned and communicated in writing?	List of writen delegations						Preventive Detective
1.1.7. The organisational chart includes segregation of tasks for incompatible functions?	Book of processes: audit trail and flowchart						Preventive
1.2. The different levels and steps of control							
1.2.1. Computerised control system is integrated within IT systems used?							Preventive Detective
1.2.2. For some transactions, an ex-ante control procedure is obligatory?							Preventive

1.2.3. For some transactions, an ex-post control system is put in place?							Corrective
1.2.4. For some transactions, a self-control system is put in place?			If yes, what are the modalities of control (exhaustive, sample, rate …)?				Detective
1.2.5. For some transactions, a four-eye control procedure is put in place?			If yes, what are the modalities of control (exhaustive, sample, rate …)?				Preventive Detective
1.2.6. For some transactions, a supervision control system is put in place?			If yes, what are the modalities of control (exhaustive, sample, rate …)?				Preventive Detective Directive
1.2.7. Some comparisons of current-period information with similar information for prior periods (from year to year, the current quarter to the same quarter last year, month to month, etc.) are made for some transactions?							Detective
1.2.8. Some transactions are reconciled with accounting information, operating information, external information?							Detective
1.2.9. Errors and irregularities detected are corrected in due time?							Detective
1.2.10. Errors and irregularities detected are collected for annual analysis and follow-up indicator (typology, figures, amounts, and activity concerned...)?							Corrective
1.3. Assets and supportive document safeguard general arrangements							

1.3.1. Is a logical security system in place (authentifi cation for accessing to IT systems, data protection and safeguarding)?							Preventive Detective
2. Documentation issues							
2.1. Existing Documentation							
2.1.1. Activity is defined and described in directives, instructions cross - referenced and at all staff disposal?							Preventive Detective
2.1.2. Activity is described in flowcharts and audit trails. These latter are regularly used by staff and updated?	Book of processes: audit trail and flowchart						Preventive Detective
2.1.3. Activity is described in detailed guidelines?							Preventive Detective
2.2. Compliance with exiting documentation							
2.2.1. Some regulation reminding are regularly made to the staff?							Preventive Directive
2.2.2. Rules are regularly updated?							Preventive Directive
2.2.3. A training system for new regulation taking over is put in place?							Preventive Directive
3.1.Participants identification							
3.1.1. For each transaction, it is possible to identify the staff involved in all steps?							Preventive Detective
3. Traceability issues							
3.2. Transactions traceability							
3.2.1. Transaction descriptions are clear and relevant?							Preventive Detective

3.2.2. Transactions archives safeguard guarantees previous years transaction traceability?							Preventive Detective
3.3. Controls traceability							
3.3.1. Self-controls are formalised with control forms?							Detective Corrective
3.3.2. Supervision controls are formalised with control forms?							Detective Corrective

MODEL OF ORGANISATIONAL / FUNCTIONAL CHART

Tasks	Person responsible	Substitute represntative	Operational supervisor	Delegation of signature	IT Systems used-authorisation	Self-control Sheet (S)	Comments
Accounting and reporting function monitoring							
Goals policy setting up (operational goals)	Head of department	Mr./Ms	Executive Management				
Department organisation							
Tasks assignment	Head of department	Mr./Ms	Executive Management				
Documentation management & information flows	Head of department	Mr./Ms					
Security of assets and IT hard systems responsibility	Each staff and the Head of Department: Mr/Ms		Executive Management				
Accounting system organisation							
Accounting evidence and bookkeeping responsibility assignment (precise accounts concerned)	Head of Department		Financial Management Controller				
IT systems access authorisation	Head of Department						
Accounting transactions / bookkeeping deadlines management	Each staff involved in the activity: Mr/Ms		Head of Department				
Accounting controls							

Tasks	Person responsible	Substitute represntative	Operational supervisor	Delegation of signature	IT Systems used-authorisation	Self-control Sheet (S)	Comments
Control of significant transactions	Each staff involved in the activity: Mr/Ms		Head of Department, the Deputy and the Financial Management Controller				Sensitive / material transactions included
Control of re-bookkeeping	Head of Department	Mr./Ms	Financial Management Controller				
Control of accounting misstatements	Head of Department	Mr./Ms	Financial Management Controller				
Control of adjustment between the main accounting and the sub-accounting systems	Each staff involved in the activity: Mr/Ms		Head of Department, the Deputy and the Financial Management Controller				
Control of the trial balance and of contra accounts	Each staff involved in the activity: Mr/Ms		Head of Department, the Deputy and the Financial Management Controller				
Clearing accounts (or suspense accounts) follow-up	Each staff involved in the activity: Mr/Ms		Head of Department, the Deputy and the Financial Management Controller				

ANNEX No 6

MODELS OF CONTROL SHEET

6.1. INTERNAL CONTROL SHEET

Person 1 accountable for control (P1)		Person 2 accountable for control (P2)	
Name		Name	
Unit		Unit	
Function		Function	
Date		Date	
Signature		Signature	

INSTRUCTIONS :

- All persons assigned to perform controls must, for each control, tick the boxes using: √ за **„OK"**, **X** за **„No or N/A for not applicable"** in the column corresponding to their respective position.
- Comments / notes may be added on the last page of the Check-list and must be cross-referenced (numbered) in the column "Note Ref. "
- The check-list must be signed by the performers of controls and reviewers once all controls are performed

Activity/ task	Control	Preventive action to be checked	Risk level	Check:% or all	P1	P2	Note ref.
1.1	01				☐	☐	
1.1	02				☐	☐	

NOTES / COMMENTS / INSTRUCTIONS:

Person 1 in load of control
Reference (to be reported in the column Note Ref) and Content of the notes / comments / instructions:

Person 2 in load of control
Reference (to be reported in the column Note Ref) and Content of the notes / comments / instructions:

Internal auditor
Reference (to be reported in the column Note Ref) and Content of the notes / comments / instructions:

	Other			
Reference (to be reported in the column Note Ref) and Content of the notes / comments / instructions:
This area is dedicated to comments / notes / references / etc... of internal auditors
Ref	**Date**	**Name**	**Comments**	**Signature**

6.2. SELF CONTROL FORM

> **Self-control form**
>
> **Process / activity / task**
>
> **Foreign Currency Payment Operations/Treatment of the payment request/Control of accuracy and validity of foreign exchange payment concerning the payment request**

Frequency

Daily	Weekly	Monthly	Semester	Annual
Other: At each payement request				

Nature and type of control

Self-control	Nature: regularity control

Control objectives

Having the insurance of paying on the basis of a valid payment request

Description of the way to implement the control

Checkin g the validity of the documents: signature, conformity of request of payment with supporting documents (invoices, contracts) and Treasury system. The control must be done before due date or at due date (at the outside) in case of late receiving.

Documents required implementing the control

Paymen t request, list of signature of authorised people, invoices and contracts, Treasury data, institutional framework in Book of processes.

Person in charge of the control

6.3. EX POST SUPERVISION CONTROL SHEET

MAIN CONTENTS		
Process		
Activity		
Process Owner (Responsible Entity)		
Name of the official in charge of the supervision control		
Kind of control	Control objective	Origin of control request
Date of control	Date of previous supervision control	Statements and documents used for the control
DD/MM/YYYY	DD/MM/YYYY	
SAMPLE and CONTROLS		
Number of operations controlled	Selection criteria	Amount of activities controlled
CONTROL RESULTS		
No anomaly detected	☐	Anomaly(ies) detected	☐ √

Description of anomalies detected

Detected anomalies causes

Organisational causes	
Documentation causes	
Traceability causes	

Date of anomalies resolution	DD/MM/YYYY	Comment	

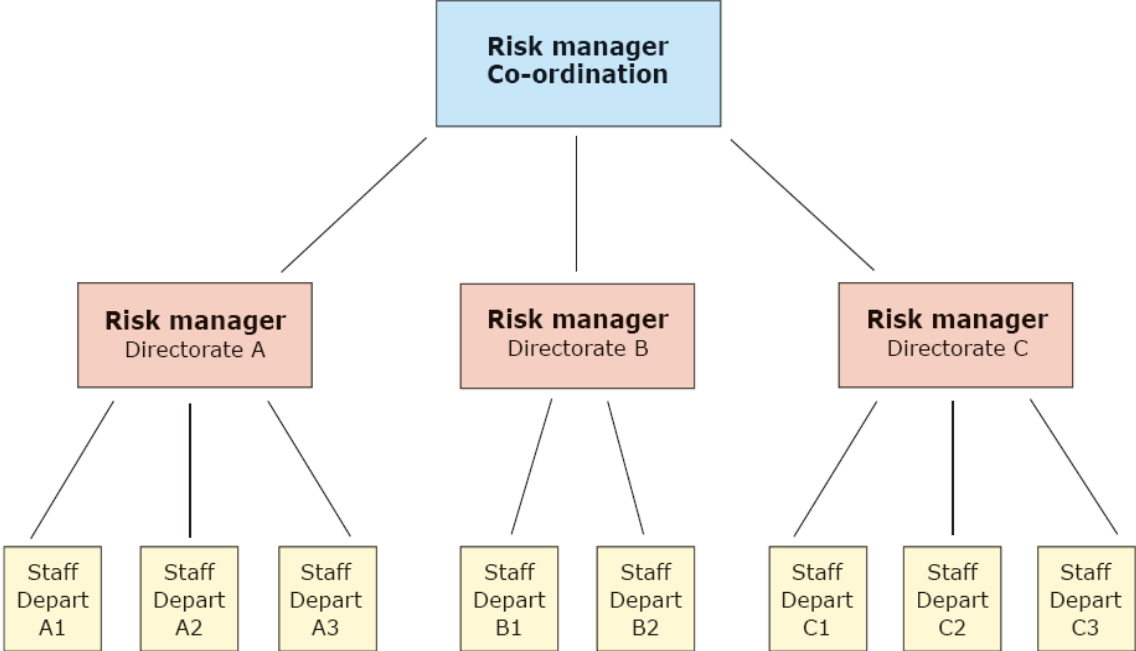| FOLLOWING OF THE CONTROL	
Instruction recall to persons in charge of the task □ √	Action to be implemented □
Description of the action to be implemented	

SIGNATURE

MODEL OF ACTION PLAN FOR WEAKNESSES ELIMINATION

Risk Mapping Scale reference	Proces Identification	Activity	Risk caregory	Detected Risk	Comments on detected risk	Action	Responsability (key responsible persons)	Deadline (Month/Year)	Completed ? (Y/N)	Risk active /close ? (A/C)
2009-BP-01	Budget preparation	Fiscal impact assessment of legislation and international treaties and agreements	Organisational	Ministry of Finance does not put in place annual or multiyear performance indicators	This is being developed for the whole state budget					
			Documentation							
			Traceability							
2009-BP-02	Budget preparation	Budget Preparation Process and Local Authorities Budget	Organisational							
			Documentation							
			Traceability							

RISK MANAGEMENT ORGANISATIONAL CHART

ACTIONS	ORGANISATIONAL CHART	TOOLS
Consolidation		Risk Mapping
Corroboration		
Review	Risk manager Co-ordination	Consolidated action plan
Reporting		Annual report
Monitoring		
Supervision	Risk manager Directorate A — Risk manager Directorate B — Risk manager Directorate C	Risk assessment form
Approval		
Updating		Directorate action plan
Updating	Staff Depart A1 — Staff Depart A2 — Staff Depart A3 — Staff Depart B1 — Staff Depart B2 — Staff Depart C1 — Staff Depart C2 — Staff Depart C3	Book of processes
Self assessment		Risk assessment form

FIRST AND SECOND LEVEL OF CONTROL ACTIVITIES

1/ First level controls: Working unit's level

Nature of controls	Ex-ante / ex-post control	Persons in charge of the control	Documentation used	Traceability	Filling
Self-controls	Ex-ante	The employee who manages the controlled operation	Self-control form	Light traceability. IT system or written identifi cation on the statements used to perform the control	IT system or the same rules as controlled statements filing rules.
Four-eye controls	Ex-ante	A different employee from the one whom initiated the operation (segregation of duties).	Four-eye control form	Light traceability. IT system or written identifi cation on the statements used to perform the control	IT system or the same rules as controlled statements fi ling rules.
Supervision	Ex-ante (final approval of an operation)	An executive (head of department, of sector…)	Instructions, directives	Light traceability. IT system or written identifi cation on the statements used to perform the control	IT system or the same rules as controlled statements filing rules.
	Ex-post (self-assessment through internal control questionnaires)		Questionnaires	Questionnaires answers	Specific filing (by the supervisor and the person in charge of internal control coordination).
	Ex-post (control of a specific operation or part of a process on a sample basis).		Instructions, directives	Ex-post supervision form	Specific filing (by the supervisor and the person in charge of internal control coordination).

2. Risk management and second level activities

▪ **The action plan management**

1. Consolidating the FMC action plan drafted by the directorates and approved by the n°1 (Risk manager co-ordinator)
2. Up-dating the action plan when a new action has been drafted by the directorates and approved by the n°1(Risk manager co-ordinator)
3. Following the deadlines and making regular reports to the n°1 about the action plan progress in accordance with the heads of directorates (Risk manager coordinator)

▪ **Control activities**

1. Proposing to the n°1 an annual program of ex-post supervision controls (in accordance with the heads of departments) and second level controls according to the main risks identified (Risk manager coordinator and person in charge of second level controls).
2. Centralising and formal analysis ex-post controls (self-assessment questionnaires and ex-post supervision controls).
3. Performing second level controls: performing corroboration controls (on the spot) according to the main risks identified. The second level controls may result in recommendations to the directorates up-dating the action plan.

▪ **Methodology**

1. Making proposals to improve the organisation of internal controls and the tools.
2. Training the staff when necessary.
3. Assist the working units to manage their risks.

ANNEX No 10

TEMPLATE STRUCTURE FOR ANNUAL REPORT

TABLE OF CONTENTS

Executive Summary

Scope of the report

Major activities

Major issues

Major recommendations and future plans

I. Introduction

    1.1. System of PIFC in the Republic of Macedonia

    1.2. Purpose of the report

    1.3. Legal basis of the report

    1.4. Material basis of the report

    1.5. Coverage of the report

    1.6. Reference

II. General part - Findings

2.1. Proper Financial Management and Control strategy

    2.1.1. Financial control system mechanisms

    2.1.2. Risk management strategy and policies

2.2. Assessment of FMC system implementation

    2.2.1. Financial Management and Control system organisation

    2.2.2. Implementation of activities for Financial Management and Control

    2.2.3. Performance of Financial Management and Control system

    2.2.4. Follow-up audit recommendations

  2.3. Proposals for the development of the Financial Management and Control system

 III. Specific part

    3.1. Financial management and control self-assessment questionnaire

    3.2. Maturity level of fiscal risk management

IV. Signature and date

Used materials

- *"Risk Management Guidelines" Croatia, June 2009 , Phare 2006 Project "Developing Public Internal financial Control in the State Treasury" financed by European Union.*