IPA TWINNING PROJECT „SUPPORT TO EFFICIENT PREVENTION AND FIGHT AGAINST CORRUPTION “

This project is funded by the European Union, and is implemented by the State Commission for Prevention of Corruption from the beneficiary country and the Federal Office for Administration from Germany

CORRUPTION RISK MANAGEMENT:

Addendum to the Risk Management Guidelines

Jure Škrbec, Ph.D

Skopje

September, 2016

Acknowledgment

This document was prepared in collaboration of State Commission for the Prevention of Corruption and Jure Škrbec, Ph.D., expert, within the course of Twinning Project "Support to efficient Prevention and Fight against Corruption". Project is funded by the European Union.

The views expressed by expert, Jure Škrbec, Ph.D., within this project are purely those of the author and may not in any circumstances be regarded as stating an official position of office where he is currently employed. He attends this project not based on his office involvement but as an international independent expert. All used sources are publically available information on the internet and of expert's experiences/knowledge.

Source of picture on the cover page: *https://shortcourses.iwcollege.ac.uk/courses/employer-training/level-2-award-risk-assessment/*

PRELIMINARY REMARKS

The nature of this document is to serve to the public sector institutions and their employees in order to give them assistance in identifying corruption and other unethical risks. It represents a supplement to the current Risk Management Guidelines adopted and updated by Public Internal Financial Control Department of Ministry of Finance of the beneficiary country in March 2015.

However, this document is not introducing new process or supplement methodology only for corruption risk management but uses already identified and accepted method by the Law on Public Internal Financial Control (hereinafter LPIFC) and Risk Management Guidelines.

Besides, handbook is not focusing on all processes within methodology for risk management but only on the phases how to identify corruption risks.

1. INTRODUCTION

According to different research and analysis it was identified that corruption represents a major problem in the Beneficiary country and it is perceived to be spread in all levels and areas of the country. Corruption is ranked as the fifth top problem in the country after unemployment, poverty, low incomes, and high prices. For years, numerous polls showed that corruption was considered as one of the top three problems in the society of the beneficiary country. There are differences between perceptions and experience (victimization). While customs officers, judges, ministers, and tax officers are perceived as the most corrupt, on the other hand, professions such as doctors, local authorities, police officers, and university professors are those who are actually most corrupt (USAID, 2014)[1].

Due to the mentioned state of play of corruption in beneficiary country, representatives of institutions needs to consider implementing effective Corruption Risk Management (hereinafter CRM) since this method represents the most effective prevention tool to minimise corruption within countries.

For institutions to be able effectively manage its corruption risks, the risks must be first **identified** and then **analysed** using a risk assessment process. If performed and used correctly, a CRM can be a powerful proactive and preventive tool in the fight against corruption in each and every (public or private) institution. The most important thing, which is often misunderstood, is that almost any kind of risk presents also possible threat for the occurrence of corruption. For example: lack of personnel can endanger effectiveness of institution and it is pure HR issue, but on the other hand, such risk can present also danger for corruption since lack of personnel means also overloads for one (few) person(s), backlogs and excessive concentration of power and decision-making process (lack of controls etc.). In this manner, some cases / tasks could be put on side deliberately (statute of limitation) or some cases/tasks could be solved first (distribution of funds) or decision-making without proper control.

CRM is a process aimed at proactively identifying and addressing an institution's vulnerabilities to both internal and external threats - illegal or unethical behaviours. As every institution is different, the corruption risk assessment process is often more an art than a science. There is no one-size-fits-

[1] USAID Corruption Assessment Report. Available at: http://seldi.net/fileadmin/public/PDF/Publications/CAR_Macedonia/CAR_MacedoniaEnglish.pdf

all approach (on the other hand legislation and rules should be the same for all institutions in the country). However public institutions have some common issues – areas (HR, public procurement, protection of data, etc.) which can be approached in a similar way. What is more: institutions with same basis or nature of work (local governments, ministries, independent state authorities, prosecution services, courts, educational institutions, health institutions etc.) could have even similar processes and tailored made approach (and trainings).

Objective of each corruption risk assessment starts with an identification and prioritization of corruption risks to help an institution recognize what makes it most vulnerable to corruption. Through a corruption risk assessment the institution is able to identify where corruption is most likely to occur, enabling proactive measures to be considered and implemented to reduce the chance that it could happen. What is more, the corruption risk assessment process should be visible and communicated through the institutions. Employees will be more inclined to participate in the process if they understand its purpose and the expected outcomes. That is why it is important to train responsible persons in institution how proper corruption risk assessment should be done and prepared.

2. WHY INTRODUCING CORRUPTION RISK MANAGEMENT AS AN ADDENDUM TO THE CURRENT LEGAL FRAMEWORK OF RISK MANAGEMENT

Beneficiary country has on the national level some strategic documents and acts for Risk Assessment management. On the other hand, on the institutional level, it has in place system regards risk assessment and risk management according to the Law on Public Internal Financial Control. Mentioned law, although it is in majority of financial nature, it has wide defined terms, conditions and methodology also to cover corruption risks, **so in that sense beneficiary country does not need another, separate corruption risk management system**.

However, six years after adopting mentioned law, implementation of its provisions **remains very weak**. In average about 50% of all central public institutions and approximately 25% local institutions adopted their Risk assessment Strategies and Actions plans although this is obliged by the law. Due to the mentioned and due to the lack of effective sanctions, mandatory regulations, lack of national coordination and lack of uniform method and forms for all institutions (based on a law) **there is question of proper and efficient system of risk assessment and risk management as it is currently set up in the beneficiary country**.

System as such (meaning methodology, forms and guidelines) should be in this regard strengthened and should be up-dated also with following issues: corruption and fraud issues (definitions), law-binding system of (Corruption) Risk Management to be the same for all institutions, identification of national independent body for the control, coordination and analysing of corruption risks, adopting effective sanctions (if risk assessment is note properly done, if risk register is not send to the competent body(ies), etc.) and up-dating (also making simpler and practical, especially user-friendly) current Guidelines on Risk Management and its attached forms/samples with indicators for the corruption and fraud risks with better method and process for identifying risks within institutions.

Simple reason for this update is that LPIFC and Risk Management Guidelines are focusing on strict financial issues, where examples and forms are too financially narrowed **although definition of risk is very wide** and covers any kind of potential threat. If institutions in the Beneficiary country want to achieve more efficient work with regard the Risk Management (**so to identify also other non-**

financial risks), then examples, forms and templates need also description of general issues (not to give only financial examples as it is currently a case). This document is especially prepared for this reason – so that risk management will be more wide and general for all risks, not only for financial (including especially examples of corruption risk).

In this way public officials within public sector institutions would be warned about obligations and corruption (and fraud) risks and how to identify them.

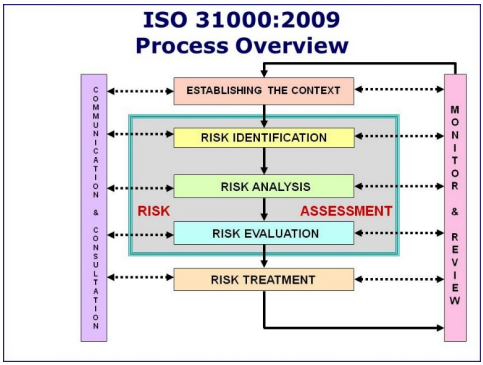
3. INTERNATIONAL STANDARDS AND BEST PRACTICES REGARD CORRUPTION RISK MANAGEMENT

3.1 International standards

There are several international standards which are defining and dealing with the CRM, as follows:

3.1.1 Australian and New Zealand risk management standard: AS/NZS ISO 31000: 2009[2]

The process of risk assessment methodology can be shown by following picture which is self-explanatory and provides recommendable process of proper CRM:



The Standard is supported by the:

- International Standard ISO/IEC 31010:2009–Risk Management;
- IEC/FDIS 31010 Risk Management–Risk Assessment Techniques; and
- ISO Guide 73:2009–Risk Management–Vocabulary.

3.1.2 Australian standard AS 8001-2008 - Fraud and Corruption Control

Mentioned standard provides entities with the tools they need to apply general risk management principles to the control of fraud and corruption. As noted by Selinšek (2015:33[3]), the Standard proposes an approach to controlling fraud and corruption through a process of:

- establishing the entity's fraud and corruption control objectives and values;
- setting the entity's anti-fraud and anti-corruption policies;

[2] Available at: http://www.finance.gov.au/sites/default/files/COV_216905_Risk_Management_Fact_Sheet_FA3_23082010_0.pdf

[3] Available at: http://www.rcc.int/download/pubs/CRA_in_public_ins_in_SEE-WEB_final.pdf/23694383579529dc40cfc2346aa3626e.pdf.

- developing, implementing, promulgating and maintaining an holistic integrity framework;
- fraud and corruption control planning;
- risk management including all aspects of identification, analysis, evaluation treatment, implementation, communication, monitoring and reporting;
- implementation of treatment strategies for fraud and corruption risks with a particular focus on intolerable risk;
- on-going monitoring and improvement;
- awareness training;
- establishing clear accountability structures in terms of response and escalation of the investigation;
- establishing clear reporting policies and procedures;
- setting guidelines for the recovery of the proceeds of fraud or corruption;
- and implementing other relevant strategies.

3.1.3 COSO standard

According to an updated COSO standard/methodology from 2013[4] there should be 17 principles to meet in every institution, as follows:

Control Environment *– 5 Principles*

1. *Organization demonstrates a commitment to integrity and ethical values.*
2. *Top management demonstrates independence and exercises oversight of the development and performance of internal control.*
3. *Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.*
4. *Organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.*
5. *Organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.*

Risk Assessment *– 4 Principles*

6. *Organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.*
7. *Organization identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.*
8. *Organization considers the potential for fraud in assessing risks to the achievement of objectives.*
9. *Organization identifies and assesses changes that could significantly impact the system of internal control.*

Control Activities *– 3 Principles*

10. *Organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.*
11. *Organization selects and develops general control activities over technology to support the achievement of objectives.*

[4] Available at: http://www.protiviti.com/en-US/Documents/Resource-Guides/Updated-COSO-Internal-Control-Framework-FAQs-Second-Edition-Protiviti.pdf

12. *Organization deploys control activities through policies that establish what is expected and procedures that put policies into action.*

***Information and Communication** – 3 Principles*

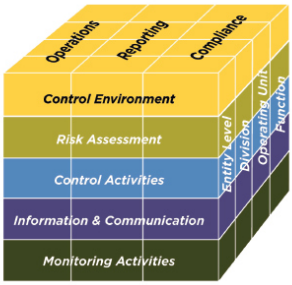
13. *Organization obtains or generates and uses relevant, quality information to support the functioning of internal control.*
14. *Organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.*
15. *Organization communicates with external parties regarding matters affecting the functioning of internal control.*

***Monitoring Activities** – 2 Principles*

16. *Organization selects, develops, and performs on-going and/or separate evaluations to ascertain whether the components of internal control are present and functioning.*
17. *Organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.*

Picture below shows process of COSO methodology

COSO Cube



3.1.4 United Nation's Convention against Corruption (UNCAC)

UNCAC advises parties to act towards sound anti-corruption strategies and measures, amongst which CRM is also included in following ways. Each State Party shall:

- enhance awareness of the **risks of corruption** inherent in the performance of public officials functions (Article 7),
- take appropriate measures to promote transparency and accountability in the management of public finances, amongst other also effective and efficient systems of risk management and internal control (Article 9),
- take such measures as may be necessary to enhance transparency in its public administration, including also publishing information on periodic reports on the risks of corruption in its public administration (Article 10).

3.1.4.1 Technical Guide to UNCAC[5]

Technical Guide to UNCAC recommends that States Parties should design the strategy to prevent corruption on the basis of a risk assessment that should be founded on relevant information or statistical data. Useful data may include audit reports and other research / studies / reports. The information and data should form the basis of a risk or vulnerability assessment that identifies the trends, causes, types, pervasiveness and seriousness or impact of corruption. This will help develop a better knowledge of the activities and sectors exposed to corruption, and the basis for the development of a preventive strategy, buttressed with relevant policies and practices for better prevention and detection of corruption. The aim of risk assessment is according to this Technical Guide to UNCAC to prepare a report addressing the assessments and specific risks within vulnerable sectors, with consequential proposals to deal with them.

3.1.5 OECD Public Sector Integrity – A framework for assessment[6]

As Selinšek warned (2015)[7] OECD methodology was mostly developed as a step further from the corruption risk assessment, i.e. assessment of the public sector policies promoting integrity and preventing corruption. According to the OECD methodology, the "assessment journey" starts with identifying which building blocks of an "ethic infrastructure" (the institutions, systems and mechanism for promoting integrity and preventing corruption in the public service) need to be assessed. An assessment may focus on separate specific measures and their interaction, in particular:

- risks (analysing risks and reviewing vulnerable areas susceptible to corruption),
- specific policy instruments (assessing discrete integrity and corruption prevention measures),
- complex programs (examining the interaction of combined policy instruments),
- elements of an organizational culture (reviewing values, behaviours and specific individual actions).

When assessing integrity and corruption prevention measures, public organizations face a variety of challenges that need to be addressed in following steps:

Step 1. Defining the purpose: Why assess?
Step 2. Selecting the subject: What to assess?
Step 3. Planning and organizing the assessment: Who will assess?
Step 4. Agreeing on methodology: How to assess?
Step 5. Ensuring impact: How to integrate assessment results into the policy cycle?

In short terms, there are four phases for corruption / integrity management according to OECD:

- definition of the integrity framework
- assessment and evaluation of the threats, risks
- application of the results
- follow-up and accountability.

In a process of risk analysis institution should:

- map sensitive processes (e.g. procurement, promotion of staff members, etc.)

[5] Available at: https://www.unodc.org/documents/corruption/Technical_Guide_UNCAC.pdf
[6] Available at: http://www.keepeek.com/Digital-Asset-Management/oecd/governance/public-sector-integrity_9789264010604-en#page1
[7] Available at: http://www.rcc.int/download/pubs/CRA_in_public_ins_in_SEE-WEB_final.pdf/23694383579529dc40cfc2346aa3626e.pdf

- map sensitive functions (typically staff-members with a responsible role) and
- identify the points where there is a significant vulnerability for integrity violations.

3.1.6 USAID Anti-corruption Assessment Handbook[8]

In contrary to above mentioned standards this Handbook gives detailed description of each phase and the activities within it, including substantial guidelines on corruption and its features which is why it is recommendable using this reading for further assistance in practice.

3.1.7 United Nations Global Compact Management[9]

Similar model is also UN Global Compact Management model which assists companies / institutions in achieving higher levels of performance and integrity over time. This model defines further actions regards risk assessment:

1. Establish the process
    a. The objective is to provide a structured approach to conducting an anti-corruption risk assessment at an enterprise by following all mentioned steps (1-6) (planning, objectives, stakeholders, and resources).
2. Identify the Risks
    a. Exploring the principles, techniques, and practices that can help an enterprise identify risk factors.
        i. Data collection (desktop research, interviews, surveys, workshops)
        ii. Processes
3. Rate the risks
    a. Probability of occurrence (high, medium, low)
    b. Potential impact (high, medium, low)
        i. Usage of temperature map
4. Identify and rate measures to minimize risks:
    a. Identify different frameworks,
    b. Rating measures (effective, partially and not effective)
5. Calculate residual risks
    a. Residual risk is the risk that remains after controls (measures) are taken into account
6. Develop action plan to address the risks
    a. Response to residual risks (current risks) which contains:
        i. Action
        ii. Responsible person
        iii. Implementation timetable.
        iv. Estimate of resources need to address each action item, such as number of individuals, hours and budget

3.1.8 UNDP (United Nations Development Programme)

The UNDP risk management policies and procedures establish a five-step process as follows:

- The identification and classification of risks;

[8] Available at: http://pdf.usaid.gov/pdf_docs/pnadp270.pdf
[9] Available at: https://www.unglobalcompact.org/docs/news_events/9.1_news_archives/2010_06_17/UN_Global_Compact_Management_Model.pdf

- The measurement and evaluation of these risks;
- The prioritization and ranking of risks in relation to each other;
- The development of a risk management plan applicable to each programme;
- The development of a programme of monitoring and follow-up.

3.1.9 INTOSAI (2004)[10]

Integral process that is affected by an entity's management and personnel and is designed to address risks and to provide reasonable assurance that in pursuit of the entity's mission, the following general objectives are being achieved:

- executing orderly, economical, efficient and effective operations,
- fulfilling accountability operations,
- complying with applicable laws and regulations,
- safeguarding resources against loss, misuse and damage.

It is similar process than COSO / ISO 31000 composed of following phases:

- establishing and identifying control environment,
- risk assessment,
- control activities,
- information and communication,
- monitoring.

3.1.10 SELF-ASSESSMENT INTEGRITY (SAINT MODEL)[11]

Model developed by Netherland's Court of Audit. It is based on following 5 steps:

1. Identification and assessment of areas of vulnerability inherent to the activities and processes of the organization (they can include contracting, document issuing, legislative activities, law application, relationships with private sector, management of state property, etc.);
2. Assessment of the factors increasing vulnerability (such as increasing complexity of work, rapid legal or other changes, management and personnel),
3. Assessment of the integrity-based control system (with the aim of establishing how resilient the individual organization is in terms of arising corruption risks);
4. Deviation analysis (aimed at establishing whether the balance between the vulnerability profile determined in steps 1 and 3 and the level of the integrity-control system (step 3) is sufficient);
5. Follows only if step 4 shows insufficient balance between the identified vulnerability and control-system. In this case, based on the results of the deviation analysis, a plan is prepared on how to manage the most dangerous processes and what measures are required to improve organization's resilience against corruption risks.

3.2 COUNTRIES' BEST PRACTICES WITHIN EUROPEAN UNION AND BEYOND

In the literature and within EU discussions and evaluations only three countries are identified as leading countries in the area of Corruption Risk Assessment Management. In Central and Eastern part of EU level, first best practice was identified in Slovenia, but in wider area there are also Netherlands and Australia, the last mentioned as an ice-breaking country regards Corruption risk

[10] Available at: http://www.intosai.org/issai-executive-summaries/view/article/intosai-gov-9100-guidelines-for-internal-control-standards-for-the-public-sector.html

[11] Available at: http://www.intosaijournal.org/technicalarticles/technicalapr2008b.html

management. We will point out the **Australian** and **Slovenian** models by visualizing them in following way:

Australia:

Process of CRM **Based on: ISO 31 000 standard**	• Identifying the risk • Analysing the risks • Evaluating the risks • Treating the risks • Amending existing controls • Introducing new controls • Introducing new methods of detecting corrupt behaviour Implementing the risk management approach	
Product of CRM	**Corruption risk treatment plan:** • proposed actions (measures to minimise the risks) • resource requirements • responsibilities (identify responsible persons) • timeframes • reporting and monitoring requirements	
Tools for identifying risks and other information	• Past organisational experience • Annual audit results • Internal investigation reports • Results of audits / physical inspections • Records of prior losses • Staff and client/customer complaints. • Questionnaires and interviews • Surveys • Observing workplace activities • Brainstorming	
Up-dating the plan	Risk assessment should be repeated every three years	
Recommendable/obliged tool	Recommendable; not obliged by the law	
Sanctions and controls	None	
Responsible person	**Institutional level**: - Working group	**National level**: - Independent State AC Commission

Slovenia:

Process of CRM **Based on:** • Victorian Managed Insurance Authority (VMIA • Australian/New Zealand Standard (AS/NZS 4360: 2004). • A methodology used by Slovenian government auditors for controlling financial risks • INTOSTAI and COSO methodology • Balanced Scorecard (BSC)	• Identifying the risk • Analysing the risks • Evaluating the risks • Treating the risks • Amending existing controls • Introducing new controls • Define responsible persons and deadlines for the treatment of risks • Implementing the risk management approach

Product of CRM	**Integrity plan:** • Assessment of corruption exposure of the institution • Identifying personal names and work posts of the persons responsible for the integrity plan • Includes a description of organisational conditions (O), staff (E) and typical work processes (P) including a corruption risk exposure • Assessment and proposed improvements regarding: - the quality of regulations, management, administration - the integrity of staff and institution - transparency and efficiency of processes and - measures for timely detection, prevention and elimination of corruption risks.	
Tools for identifying risks and other information	• Past organisational experience • Annual audit results • Internal investigation reports • Results of audits / physical inspections • Staff and client complaints • Surveys • Brainstorming	
Up-dating the plan	Risk assessment should be repeated every year	
Recommendable/obliged tool	Obliged by the law	
Sanctions and controls	None	
Responsible person	**Institutional level**: - Working group and - Integrity manager	**National level**: - Independent State Commission for the Prevention of Corruption

3.3 International standards and best practices – different or common practices and standards?

- Different methodologies (ISO 31 000, COSO, SAINT, OECD etc.) and different ways (internal auditing, self-assessments) are used in countries and international organisations, but all approaches have the same goal: **to reach, promote and to maintain integrity within institution(s) through eliminating risks and vulnerabilities**.
- Countries that have established integrity (risk) management tools have done it through laws or different (government) decisions,
  - anti-corruption laws spells out which institutions are required to implement such tools,
  - central and independent state bodies for counselling and control,
  - unique and obliged (law-based) guidelines and methodology for all institutions,
  - standardisation for benchmarking corruption risks across country(ies),
  - unique and law-based monitoring process.
- Identified person in each institution – integrity manager/officer by law,
  - responsible person for implementation of integrity plans / action plans,
- Mandatory tools and processes to gain final result (uniform process, methods and results),
- Sanctions for public institutions when not adopting or not implementing required measures/plans,
  - Sanctions for responsible persons (head of institution, integrity managers/officers),
- Lack of IT solutions.

4. RECOMMENDABLE BASIS AND APPROACH FOR CRM (COMBINATION OF INTERNATIONAL BEST PRACTICES AND STANDARDS AND THE BC SYSTEM)

After reviewing all best practices and international standards and having in mind the methodology of the beneficiary country, we could recommend following issues and recommendation to do proper and efficient **corruption** risk assessment and management.

4.1 Defining terms

First of all, country needs to define all necessary terms. This represents basic for further work. Currently in the Beneficiary country there are definitions of following terms:

> ***Corruption*** *means misuse of office, public authorization, official duty and position for the purpose of gaining any benefit for oneself or others (Article 1-a of the Law on Prevention of Corruption);*
>
> ***Risk*** *as the probability of occurrence of event with a negative impact on the achievement of the objectives of the entity (Article 3/24 of LPIFC);*
>
> ***Risk management*** *as a process of ascertaining and assessing the internal and external risks which may negatively affect the fulfilment of the objectives of the entity and the implementation of the necessary controls in order to keep the exposure of the risks to an acceptable level or to decrease the consequences of possible risk to an acceptable level (Article 3/25 of LPIFC);*
>
> ***Suspicion of fraud*** *which means undertaken or not undertaken act, from which, one can excusably bring a conclusion for intentional or wrong presentation of the material or financial facts (Article 3/42 of LPIFC).*

What is missing is to define what corruption risk means. We propose using following definition:

> ***Corruption risk*** *is any kind of internal or external weakness or a process which may present opportunity for corruption to occur within public sector institution and includes following issues: conflict of interest, incompatibility of functions, receiving gifts and other illegal payments, lobbying, whistleblowers' protection, frauds, improper use of authority, financing political parties and campaigns, discretion power, nepotism, restrictions of operation, revolving doors, disclosing assets declarations, trade with information, transparency of procedures and documents, etc.).*

4.2 Defining process and methodology for corruption risk management

The beneficiary country has a proper methodology and process for risk assessment/management already in place (however, it does need major simplifications, some up-dates and changes, but the basis is proper and in accordance with the international standards), that is why there is no need for separate methodology or process for corruption risk management. In this sense we recommend using the Risk Management Guidelines and LPIFC when conducting and implementing process, methodology and proposed final forms / reports.

4.3 Step by step approach for identifying corruption risks

According to the mentioned, leading standards (ISO 31000:2009, COSO, INTOSAI, etc.), international guidelines (OECD, UNDP and USAID) and countries' best practices (Australia, Netherlands and Slovenia)[12] following steps should each corruption risk management process have:

a) Establishing the context ,
b) Identification of (internal and external) risks,
c) Analysing the risks
d) Evaluating the risks
e) prioritizing the risks
f) identification of control measures
g) implementation of control measures and
h) monitoring the implementation / process

Since similar steps (methodology and processes) are already in place in the Beneficiary country[13], we will focus **only and explicitly how to easily and effectively identify also corruption risks and other unethical behaviours within current legal framework.** We will show this in simplified methodology / process with 6 steps (it is based on the BC system, with only difference that it is more simplified[14]) as follows:

Step 1 - Preparatory phase

a) Decision and commitment by the top management of the institution to identify also corruption risks,
   - it is recommendable that the decision to such assessment is not left to the institutions and their management, but rather obliged by a law (or Guidelines),
   - top management should be keen, focused and prepared to do proper CRM since this procedure is important for the efficiency and integrity of institution; besides, the most important is that top management believe in such tool and shows its commitment for such process (in such way also employees will show more enthusiasm and will put more energy into this).
b) Formal and written decision and appointment of Risk Managers and Risk Management Coordinators with the defined obligation to identify and work also on corruption related risks,
c) Defining tasks and planning the work of responsible persons,
   - Development of the program/plan[15] with timeframe of different processes,
   - Defining different methods of work to identify corruption risks (Brainstorming, Focus groups, Questionnaires, Interviews, Case studies, Literature reviews, usage of indicators, etc.).
d) Gathering information,
   - Necessary to collect documentation for further tasks through the analysis of: regulations, legal framework, internal rules and procedures, internal controls and audit (external

[12] Mentioned three countries were identified as best practices regard Corruption Risk Assessment according to the Regional Anti-corruption Initiative's newest publication: *Corruption Risk Assessment in Public Institutions in South East Europe: Comparative Study and Methodology*. Available at: http://rai-see.org/focus/corruption-risk-assessment-in-public-institutions-in-south-east-europe-comparative-study-and-methodology/.

[13] Step 1 - Describing business processes and activities of institution; Step 2 - Identification of the objectives on activities of institution; Step 3 - Inherent risk identification and 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 and Step 7 - Monitoring and reporting.

[14] International best practices are also based on very simple methodologies and processes. The reason is simple: more things are complicated, more is difficult to implement all that in practice. The beneficiary country should in our opinion make this methodology and process of risk assessment also more simple and user-friendly.

[15] The programme shall include activities and tasks that shall be carried out per phases, those responsible for the implementation of such tasks, and respective times for completion.

control) reports, citizens' complaints, situation analysis (media reports, public opinions, surveys, internal surveys of climate, annual interviews with employees), organizational charts, job descriptions (qualifications), whistleblowers' information, corruption cases, and other sources of information on the areas and work processes.

e) Informing all employees inside of institution about CRM,
   - Risk managers, coordinators and the head of the institution are obliged to acquaint the employees with the definition, objective, importance and methods of the development of the CRM. The working group may familiarize the employees through/by: at all-staff meetings; holding meetings at sectorial level, sending an e-mail to all the employees; posting a notification at an appropriate spot in the institution, etc. It is most important that employees are informed that corruption risk analysis/management is not something bad which seeks for "thieves" or "corrupt employees" but effective prevention tool which will help to make institution more effective and integrity, with good reputation and increased trust by the citizens.

Step 2 – Identification of corruption risks

The aim of this step is that responsible persons (recommendable appointed special working group (WG) composed by persons working in different areas of institution) analyses institution's internal and external situation with the aim to identify risks (vulnerabilities) for the occurrence of corruption and other illegal and unethical behaviour (where, when, why and how can something occur). This is the most important phase due the simple fact: **unidentified risks cannot be treated**.

a) Gathering and analysis of information relevant to the institution (external and internal view)

First, we need to analyse all possible sources of information which can help employees within institution to identify the weaknesses and corruption risks:

- internal controls and audit (external control) reports, citizens' complaints, whistleblowers' information, corruption cases;
- situation analysis (media reports, public opinions, surveys, internal surveys of climate, annual interviews with employees);
  - employees are important source of information due to the fact they are working with clients, implementing regulations, etc.
- regulations, legal framework, internal rules and procedures,
  - with the aim to seek for: unclear rules, lack of clarity, inconsistency of regulations, to many regulations for the same issue, lack of control, lack of sanctions,
  - all this could result in too much of discretion power, possibility of different conclusions on the same matter, working without control and supervision, etc.
- organizational charts, job descriptions (qualifications) and other sources of information on the areas and work processes.

b) Identifying areas, processes / functions and indicators for identification of all relevant risks

Secondly, following LPIFC and Risk Management Guidelines, we should identify a) core areas of the institution; b) identify all processes / functions for each area; c) identify risk factors / indicators and then d) analyse all processes with the risk factors / indicators.

Identification of areas of an institution:

GENERAL AREAS: **(Areas which are the same for all institutions)**	- Institution Management - Human Resources Management - Financial Management - Public Procurement - Document Management - Institution Security
SPECIFIC AREAS: **(Institution' special - specific competences/areas)**	- Inspection - Adoption of legislation - Issuing driving licenses - Control on incompatibilities of functions, - Spatial planning - Local Elections - Protection of natural values and goods - Etc.

Identification of processes (mapping the processes) within institutions' areas:

General Area: **PUBLIC PROCUREMENT**	- Preparation of the procurement plan - Preparation of tender documents and tendering commission - Evaluation of bids and selection of bidders - Conclusion of contract - The Contract implementation - Etc.
General Area: **DOCUMENT MANAGEMENT**	- Receiving and sorting documents - Certify(signature and stamp) documents - Expedition of documents - Preservation and archiving documents - Etc.
General Area: **INSTITUTION MANAGEMENT**	- Assessment of regulations, - Creating / implementing of a work plans - The control of the performance - Quality control Management, - Etc.
General Area: **HUMAN RESOURCES MANAGEMENT**	- Drafting a personnel plan - Preparation of Act of internal organization and systemisation and its implementation - Employment procedures - Evaluation and promotion of staff - Training and education of employees - Etc.
General Area: **FINANCIAL MANAGEMENT**	- Preparation of financial plans - Planning and execution of financial plans - The use and purchase of material and fixed assets - Etc.

General Area: **INSTITUTIONAL SECURITY**	- Physical - Technical Security - Information Security - IT Security - Etc.
Specific Area: **e.g. INSPECTIONS**	- Planning the inspections (planned / unplanned) - Appointing of inspectors who will do the inspection - Process of inspection in practice - Defining and imposing sanctions - Follow-up on recommendations - Etc.
Specific Area: **e.g. URBAN / SPATIAL PLANING**	- Regulating land use - Issuing decisions - acts - Safeguarding natural resources - Safeguarding cultural resources - Process of planning the urban plans • Public discussion of draft spatial plan • Voting - Etc.

Institutions could use also **questionnaires** for all employees to identify areas, processes, responsibilities, etc. Such practices are known in many countries, for example also in Albania[16]: Following are examples of some countries' questionnaires:

Albanian Corruption Risk Assessment Methodology Guide[17]

The following questionnaire is proposed as a means for conducting a basic corruption risk assessment or good governance risk assessment. The questionnaire, should be completed either on a self-assessment basis (by the line ministry of institution itself) or externally.

A. Organisational role

1. What are the core functions of the organisation (e.g. ministry, sub-unit within ministry)?

2. Does the organisation have a 'mission statement' or similar description of its function/role? Are staff aware of these? Do staff consider them accurate and appropriate?

3. Do the major sub-units of the organisation have 'mission statements' or a clear definition of their function/role? Are staff aware of these? Do staff consider them accurate and appropriate?

4. Do all staff of the organisation have clear job description/terms of reference and are staff aware of this?

B. Budget

5. What is the size of the organisation's budget?

6. What is the rough breakdown of spending between salaries, investment, purchases of goods and services and other types of spending?

7. What is the average size of a purchase/investment made by the organisation: are there a significant number of very large purchases/investments in an average year (or last year)?

8. What percentage of purchases/investment made by the organisation are put out to open tender?

9. How technically complex are the spending decisions made by the organisation? Who takes the more complex decisions and on what basis?

[16] Albanian approach is on the one hand simple but on the other hand effective and shows good basis for further work and up-dating with more indicators.

[17] Available at: http://www.coe.int/t/dghl/cooperation/economiccrime/corruption/projects/Albania/Technical%20Papers/PACA_TP%202%202011-Risk%20Assessment%20Methodology.pdf

10. Are spending decisions on major items highly centralised (e.g. requiring the signature of one senior official) or highly decentralised?
11. Are spending decisions on minor items highly centralised (e.g. requiring the signature of one senior official) or highly decentralised?
12. Does the organization receive income from the public or designated clients (taxation, customs levies, payments for services or rents etc.) What is the process for recording, banking and auditing these payments? In what form are such payments received?

C. Human resources management

13. How many staff does the organisation employ?
14. How many of these are employed centrally (e.g. in a ministry), and how many indirectly (e.g. public servants such as teachers)?
15. What percentage of the following categories (or equivalent categories) of your staff have the status of civil servant, what proportion are currently within the one-year probation period, and what percentage are employed on short-term contracts?:
a. Secretary-General
b. Directors of departments or directors general
c. Directors of directorates or sector/office chiefs
d. Specialists
16. Is there any monitoring and statistics to show the rate of staff turnover within the organisation. If so, what is the turnover regarded by the organisation as high, low, or about right?
17. Are there any internal recruitment guidelines in addition to the provisions of the Law on Status of a Civil Servant?
18. In what percentage of recruitments is the selection decision of the relevant superior contrary to the recommendation of the ad hoc recruitment committee, i.e. selects a candidate that was not one of those recommended?
19. Do recruitment procedures for staff in positions that might be regarded as high-risk from a corruption point of view include criteria to attempt to ensure the integrity of those appointed?
20. Are applicants for staff positions questioned/screened to ensure they do not engage in external activities or hold external interests that may conflict with or impair the proper performance of their official duties?
21. Do staff have a clear understanding of what situations constitute conflicts of interest?
22. Do new staff go through any induction process such as initial training?
23. If so, does such training cover integrity issues? Is this repeated perhaps in more specific ways on promotion or when staff move to new roles?
24. Do staff regard their training as adequate to manage the situations that they face?
25. Who is designated as the person to whom staff should turn for advice? In cases of uncertainty would they seek advice from other colleagues on an informal basis before turning to their line manager, or seek advice elsewhere?
26. Do staff feel that their salaries are adequate, just sufficient or insufficient to ensure a reasonable standard of living?
27. To what extent do staff feel valued by (i) the organisation, ii) their direct superior, in their role?

D. Procedures and decision-making processes

28. Does the organisation do any of the following?

- *a) Issue or provide items such as licenses, permits, permissions, certificates, passports or other documents to citizens or entities.*
- *b) Allocate any financial or other benefits to citizens (for example social security benefits).*
- *c) Allocate any financial or other benefits to legal entities (for example subsidies).*
- *d) Receive payments from members of the public (such as fees, taxes,*
- *e) etc).*

29. Where it does so, are there clear procedures and clear criteria for the provision of such items and/or receipt of payments?
30. Where can these procedures and criteria be found?
31. Where officials have to exercise discretion in the exercise of decisions on such items, are their clear guidelines on how they should exercise that discretion (e.g. that it should serve a particular objective)?

32. If the organisation does not make a decision on items that are the subject of an application period (e.g. for a license or permission) within the deadline defined, is the issue automatically resolved to the benefit of the citizen/entity?

33. Is the procedure for provision of such items organised in such as to minimise the number of contacts citizens need to have with the organisation or other organisations (one-stop shop).

34. Are there multiple locations at which such items may be secured (e.g. different branches of the same institution, post office, etc.) or does one office have a monopoly?

E. Record-keeping

35. Does the organisation have clear rules for the management of records and files?

36. Are individual decisions of the organisation recorded and filed according to clear rules and for a clearly defined and binding minimum period?

37. Who has access to these files, who is authorised to amend them or review them?

38. What degree of freedom of information exists with respect to the institution's files and documentation, both in terms of which decisions/files/documents are made public automatically (and how), and which ones are available on request? To what extent is such access guaranteed in practice?

F. Transparency

39. Does the organisation have a formal policy or rules on the automatic dissemination of information? Does this include automatic provision on the website of the following?:

a) Organisational structure of Ministry and contact persons
b) Ministry policies and policy documents
c) Laws and sub-legal acts
d) Draft laws and regulations
e) Procedures of relevance to citizens and legal entities, such as for applications for items mentioned in Section D.

G. Access to information

40. Does the organisation have an official clearly designated to process and respond to requests for information filed under the Law on Right to Information on Official Documents?

41. How many requests were filed last year?

42. How many requests were refused or are currently in dispute?

H. Ethics and integrity framework

43. Does the organisation have its own specific code of conduct or code of ethics?

44. Are staff informed about the existence of the Code when assuming their position?

45. How often do staff receive training on ethics?

46. Are staff familiar with the Code? What steps are taken to ensure this?

47. Are there, either in such a code, or in guidelines or other regulations or staff rules, provisions that instruct staff how to proceed in situations where they find themselves subject to a conflict of interests?

I. Accountability mechanisms

48. Do staff members have clearly-defined work procedures and routines for reporting to superiors – either on a periodic basis (e.g. weekly staff meeting) or on particular decisions or activities?

49. Is there an internal inspection or control department?

50. Approximately how many inspections/controls did the department carry out last year?

51. Is there an internal audit department?

52. What were the most important findings of the department last year?

53. How often is the organisation assessed by an external inspectorate or control body?

54. How often is the organisation audited by an external audit body?

55. Were there any important findings on the organisation by such external bodies last year (or at the last assessment)?

J. Internal notification of ethics breaches

56. Is there a formal procedure by which staff members may notify a designated official or unit of the organisation of suspected breaches of integrity or contravention of the code of conduct within the organisation?

57. Where the designated official is also the official that is the subject of the complaint, is there an alternative channel by which staff may file complaints – e.g. to an external organisation or to a higher superior?

58. Are staff informed through training of these procedures and the official/unit to whom they should file complaints?
59. Are there any mechanisms in place to protect those who file such notifications form retaliation?
60. How many cases of such notifications by staff have there been in the last 12 months, and what was the outcome of these notifications for both sides involved (the official notifying, and the subject of the notification)?
K. Complaints mechanisms
61. Are there clear procedures by which citizens may file complaints against actions of our organisation or its officials?
62. Where can these procedures be found?
63. Are decisions on complaints taken by the same person or unit in the organisation at which the complaint was directed?
64. How many complaints did the organisation receive last year?
65. How many complaints were upheld as well-founded?
L. Disciplinary procedures and sanctions
66. How many disciplinary proceedings were conducted against staff of your organisation last year in connection with breaches of ethics rules?
67. How many of these proceedings resulted in sanctions being applied?
68. What was the breakdown in sanctions applied (number of cases for each type of sanction)?
M. Vulnerable areas
69. Can you identify which areas of your organisation or its activities are most vulnerable to misconduct?
70. Has a risk analysis been conducted on your organisation to identify areas vulnerable to misconduct?
71. Does your organisation's Anti-corruption Action Plan contain specific measures to tackle these vulnerabilities?
N. Anti-corruption policies
72. Who in your organisation has formal and specific responsibility for development, implementation, monitoring and coordination of anticorruption policy?
73. Is this responsibility stated in that staff member's job description (see Question 4)?
74. Is there a working group within the organisation tasked with formulation, coordination, monitoring and reporting on anti-corruption policy?

c) Identification of corruption risks and vulnerabilities for the corruption to occur

When all areas and their processes are identified, than we should identify all possible risks and vulnerabilities within each and every process. There are many ways how to do it but in general following three possibilities / ways are most common:

a) to brainstorm with working group about risks and vulnerabilities and using results of analysis of all relevant information, legislation, relevant databases, media reports, audit and control reports, etc.,
b) to assess all processes with in advance identified risks – indicators,
c) combination of a) and b).

For sure one will argue that option b) is the easiest, time saving and effective method. We could agree if all possible indicators are identified and working group is only checking if risks are present in their processes or not. Unfortunately this is almost impossible – meaning that is impossible to identify all indicators for the assessment of processes. If institution is using "only" given indicators, that means on the other hand that institution will not assess and identify all risks due to the fact they will assess processes only with identified indicators and nothing more.

That is why we suggest firstly to make proper and quality in-depth analysis of all relevant information (internal, external controls and audit reports, citizens' complaints, whistleblowers' information, corruption cases, media reports, public opinions, surveys, internal surveys of climate, annual interviews with employees, regulations, legal framework, internal rules and procedures, organizational charts, job descriptions (qualifications) and other sources of information on the areas and work processes) with the aim to search for all vulnerabilities and risks. After that we should assess the processes also with risk indicators.

How to identify risk indicators?

The Risk Management Guidelines of the beneficiary country already have basis for such an answer since it identifies 8 different groups of risks which are relevant for all institutions. Those are:

- **Strategic Risks:** 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 Risks**: 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 Risks**: (ex: lack of identified substitute, insufficient supervision arrangement / insufficient or inappropriate delegation of tasks/ inappropriate segregation of duties…);
- **Compliance Risks**: 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 Risks**: (ex: no goal monitoring system);
- **Financial Risks**: these concern the effective management and control of the fi nuances of the institution such as fraud or irregularity, and the effect of external factors such as foreign exchange rate;
- **Reputation Risks**: (ex: negative external assessment);

What is missing are fraud and **corruption Risks.** Since this Handbook is not about above mentioned 8 groups of risks[18] but only on corruption related issues, we will focus only on last mentioned – corruption risks.

As already defined in the text above corruption risks should represent: *any kind of internal or external weakness or a process which may present opportunity for corruption to occur within public sector institution and includes following issues: conflict of interest, incompatibility of functions, receiving gifts and other illegal payments, lobbying, whistleblowers' protection, frauds, improper use of authority, financing political parties and campaigns, discretion power, nepotism, restrictions of operation, revolving doors, disclosing assets declarations, trade with information, transparency of procedures and documents, etc.).*

[18] However, we recommend that Ministry of Finance identifies as many as possible indicators for each 8 Groups of risks. This will save time and make system and process more meaningful and effective.

As such, corruption risks can be divided on following **sub-risks**:

- conflict of interest,
- gifts,
- incompatibility of functions,
- lobbying,
- whistleblowers' protection,
- discretion powers (improper use of authority),
- disclosing assets declarations,
- frauds,
- revolving doors,
- nepotism,
- abuse of office,
- bribery.

Now for each corruption sub-risks we should identify indicators, as for example:

CONFLICT OF INTEREST

- Regulation exists but it is not being used in the institution,
- Regulation exists, though it is not comprehensible,
- Regulation exists, yet it is out of date,
- Regulation is not acknowledged,
- Employees are not acquainted with the regulation regarding conflict of interest,
- Lack of attention of public officials on the actual or potential conflict of interest,
- Using the office to achieve illegal private interest for himself or another person,
- Lack of notification of the head of the institution or commission about the existence of conflict of interest (real or potential) at the start or during employment,
- Employees do not cease their working in the matter where conflict of interest was found,
- Head of the institution does not act although he was informed of conflict of interest,
- Head of the institution does not comply with the provisions on the prevention of conflicts,
- Employees are not acquainted with appropriate actions on how to deal with conflict of interest,
- No supervision of Conflict of interest by management,
- Employees do not fill declarations of Conflict of interest,

RESTRICTIONS ON BUSINESS ACTIVITIES DUE TO CONFLICT OF INTEREST

- Regulation exists but it is not being used,
- The employees do not understand regulation,
- Employees are not acquainted with the regulation,
- Employees are acquainted with the regulation but do comply with it,
- Using the office or service to do business with entities who are subject to restriction of business,
- Employee does not cease doing business with the entity who is subject to the restriction of business,
- Doing business and contracting entities who are subject to restriction of business,
- Head of the institution does not act when alerted,

- No supervision,
- etc.

GIFTS

- Regulation exists but it is not being used in the institution,
- Regulation exists, though it is not comprehensible,
- Regulation exists, yet it is out of date,
- Regulation is not acknowledged,
- Employees are not acquainted with the regulation regarding receiving gifts and other benefits,
- Lack of attention of public officials on forms of gifts,
- Employees are not aware what kind of gift can / cannot be accepted, what is still acceptable value of gift which can be accepted, etc.
- Employees receive gifts but they do not inform superior / head of institution about this,
- Etc.

ILLEGAL LOBBYING

- Regulation exists but it is not being used,
- Regulation exists but is not understood,
- Employees are not acquainted with the regulation,
- Employees are acquainted with the regulation but do comply with it,
- Employee does not verify if the lobbyist willing to lobby in his institution is registered,
- Employee does not demand identification of a lobbyist ,
- Employee does not decline contact with lobbyist although conflict of interest had arisen,
- Employee does not report to the Commission about the prohibited conduct of lobbyists,
- Employee does not record contact with lobbyist, he is legally obliged to submit to head of his institution and the Commission,
- Cooperation with unregistered lobbyists,
- Unregistered lobbyists influencing decision-making process ,
- Omission, lack of supervision by the head,
- etc.

PROTECTION OF WHISTLEBLOWERS

- Regulation exists but it is not being used,
- Regulation exists but is not understood,
- Employees are not acquainted with the regulation,
- Employees are acquainted with the regulation but do comply with it,
- Employees do not implement measures to protect whistle blowers,
- Employees do not report unethical or illegal activities,
- Process of protecting potential whistle-blowers is not suitable for the institution,
- etc.

ETC.

Since there are many examples through the world practices regards identifying possible risks, which are also connected with corruption, we will add also more examples[19] of indicators / questions as follows:

- *Provisions (law, by-law, internal rules, guidelines, codes) for the implementing the process[20] does not exist.*
- *Provisions (law, by-law, internal rules, guidelines, codes) for implementing the process exists, but it is imprecise, contradictory, not up-to-date, incomplete, and inconsistent.*
- *The provision for implementing the process allows uncontrolled discretion power.*
- *The provision for the implementation the process does not contain provisions on liability and consequences for violating / not applying it.*
- *Application of the regulations in practices is inadequate within the process.*
- *Employees are acquainted with the regulation, but do not comply with it.*
- *There are enough personnel appointed / positioned to work on this process.*
- *Employees who are involved in this process do not have sufficient knowledge, competences to perform it.*
- *Employees do not have experiences to perform the process.*
- *None of or not updated, incomplete or imprecise job description within the processes.*
- *Employees have low level of integrity (professionalism, ethic, impartiality) in this process.*
- *Private problems affecting the job are not properly discussed and solved.*
- *No provision regards competition clause for employees.*
- *Employees are not motivated within this process.*
    - *I agree, I partially agree, I disagree, I do not know*
- *Established working practices are not implemented in accordance with the legislation.*
    - *I agree, I partially agree, I disagree, I do not know*
- *Not established proper documentation/records/minutes of the process.*
    - *I agree, I partially agree, I disagree, I do not know*
- *There is no efficient system of internal control in place.*
    - *I agree, I partially agree, I disagree, I do not know*
- *There are no guidelines or rules how to deal with "problematic" employees.*
- *There are no sanctions imposed due to the breach of procedures and rules of the process.*
    - *I agree, I partially agree, I disagree, I do not know*
- *The distribution of tasks to perform this process is not done according to the prescribed duties and responsibilities.*
    - *I agree, I partially agree, I disagree, I do not know*
- *Criteria for decision-making are not clearly defined.*
    - *I agree, I partially agree, I disagree, I do not know*
- *Third parties illegally and / or unauthorized affect the performance of the process.*
    - *I agree, I partially agree, I disagree, I do not know*
- *Third parties influence that this process is not running correctly.*
    - *I agree, I partially agree, I disagree, I do not know*
- *There are no provisions on Conflict of Interest within this procedure.*
    - *I agree, I partially agree, I disagree, I do not know*
- *There are no provisions on receiving gifts within this procedure.*
    - *I agree, I partially agree, I disagree, I do not know*
- *There are no provision on whistleblowers' protection.*

[19] All examples could be perfectly used also in Beneficiary country by all institutions. We recommend to divide them by risks groups (Strategic Risks, Operational Risks, Organizational Risks, Human Resources Risks, Compliance Risks, Performance Risks, Financial Risks, Reputation Risks and Corruption Risks) and to identify even more indicators. It should be noted also that some indicators are similar to above mentioned and also the same. Authors did not made selections in this sense.

[20] Process means identified process/function within each area (for example: planning the inspection or Preparation of Procurement Plan, etc.

- *I agree, I partially agree, I disagree, I do not know.*
- *Inadequate Internal Communication amongst employees within the process.*

For more examples of indicators and model questionnaire please see also:

- Ministry of Finance of the Beneficiary country (2015). Risk Management Guidelines: Annex - INTERNAL CONTROL ASSESSMENT QUESTIONNAIRE.
- USAID (2014): Public Financial Management Risk Assessment Framework Manual. A mandatory Reference for ADS Chapter 20. Available at: https://www.usaid.gov/sites/default/files/documents/1868/220mae.pdf
- USAID (2009): Anticorruption Assessment Handbook. Final Report. Available at: http://pdf.usaid.gov/pdf_docs/Pnadp270.pdf
- Council of Europe (2010) Project Against Corruption in Albania (PACA). Corruption Risk Assessment Methodology Guide. Available at: http://www.coe.int/t/dghl/cooperation/economiccrime/corruption/projects/Albania/Technical%20Papers/PACA_TP%202%202011-Risk%20Assessment%20Methodology.pdf
- Moldavian Methodology of Corruption Risk Assessment in Public Institutions. Available at: https://www.coe.int/t/dghl/cooperation/economiccrime/moneylaundering/projects/molico/AC/Output1.6/912%20MOLICO%20Nat%20%20Legisl%20_methodology%20of%20corruption%20risk%20assessment.pdf
- Serbian Manual for the Integrity plan Development (2012). Available at: http://www.acas.rs/wp-content/uploads/2010/07/Manual_for_Integirty_plan_developmnet.pdf.

All this examples of indicators should be now used to assess the processes if such risks are relevant or not to each and every institution – whether answers to such indicators are positive (answered with yes).

Step 3 – Analyse, Evaluate Risks and current Control measures

After we have identified all risks and vulnerabilities within the institution, we need to identify and analyse current / already existing control measures compared to identified risks. If these internal controls and measures are appropriate and effective, then the identified risks are not very likely to occur, to be serious or to have major consequences/effects. This phase (evaluation / analysis of current control measures) can be done parallel when identifying risks.

When analysing the risk factors working group / responsible person basically assess the relevance, power and efficiency of existing controls and measures. The result of this analysis is to determine whether a risk factor is:

a) controlled (measures are appropriate and sufficient),
b) partly controlled, (up-dating and supplementing the measure) or
c) not controlled (measures do not exist or are inadequate).

Partly controlled and not-controlled risk factors should be further evaluated using two factors:

- 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.

A risk heat map is a tool used to present the results of a risk assessment process visually and in a meaningful and concise way:

Heat map

IMPACT				
	Severe	Medium	High	High
	Moderate	Low	Medium	High
	Minor	Low	Low	Medium
		Low	*Medium*	*High*
		LIKELIHOOD		

Source: Risk Assessment Guidelines of the Beneficiary country, 2015

Definition of terms from heat map:

Assessment of IMPACT	Interpretation		Assessment of LIKELIHOOD	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		***Low***	The risk occurrence is unlikely or there is some knowledge of the occurred situation.
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		***Medium***	The event should occur sometimes. Previous evidence or knowledge of the occurred situation supports the likelihood of risk occurrence.
Severe	If the risk occurs, the activities are heavily disrupted. Examples: Disruption of all essential programs/services Loss of major assets		***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.

RESULTS OF DIFFERENT COMBINATIONS OF LEVEL OF LIKELIHOOD AND IMPACT:	
Low	No action needed or only pay attention to the identified risk
Medium	The risk must be observed, more prevention measures identify, control of identified measures to minimise risks, superior should be informed about risks
High	The risk must be observed all the time, as many prevention and control measures must be identified, strictly and very often control of the implementation of control measures, superior must be up-dated about issue weekly, involve external control mechanisms/institutions.

Source: Risk Assessment Guidelines of the Beneficiary country, 2015

Examples for corruption risks:

– Identified corruption risk: Conflict of Interest is not regulated.
– Current control measures: none
– Likelihood of occurrence of such risk: High, since it is local municipality and clients/customers are friends, relatives of official and official is working with clients/customers on daily basis,

- Impact / consequences of such risk: Severe, since local municipality can loss of public trust, bad media reports, loss of assets (all contract in conflict of interest will be null and void)
- Results / prioritization of risk: high – it should be treated as soon as possible, identification of supervision, segregation of duties, etc.
- Measures for the treatment of the risk: identify regulations on conflict of interest, identify process of avoidances of conflict of interests, sanctions, process for reporting of possible conflict of interest, hotlines, trainings for public officials, higher transparency of procedures, etc.

Step 4 – Prioritization of the Risks

We prioritize all the identified risk factors according to our results from the heat map. The risk evaluation process will help institutions to decide on the course of action to take (based on finding whether risk means minor, medium or high danger to the institution), including:

- whether a risk needs treatment (medium and high level risks),
- whether an activity should be undertaken and
- priorities for the treatment.

Applying the risk criteria consistently will identify those risks that need further treatment, and will result in a prioritized list of risks that require action in the current period. Treatments and countermeasures needs also exact deadlines for their implementation. In this way proper control could be applied. More about that please see in further text.

Step 5 – Identification and planning of solutions / measures / recommendations

In this phase responsible persons needs to determine the measures available for treating the risks (for those which represents medium and high danger for the institution), and implementing suitable risk treatment plans – risk registers. That means that in the Beneficiary country risk managers and the risk manager co-ordinator must prepare an action plan – strategy how to mitigate all risks.

Risks are commonly treated using one or more measures/strategies that involve:

- **avoiding** the risks (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.);
- **reducing** the risks (their likelihood of the risk occurring and their consequences if the risk occurs),
- **transferring** the risks (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); and
- **accepting** the risks (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.

Risk register / action plan to treat the risks and countermeasures

All identified risks and countermeasures must be now organized in one document – action plan / integrity plan / risk register. The measures / plan to treat the risks should include details of the:

- proposed actions (countermeasures),
- resource requirements (if any),
- responsible persons (official who will control the implementation of the measures from the plan and officials who are responsible for the implementation),
- timing (deadlines for implementation of all measures),

- reporting and monitoring requirements (how, when and to whom report).

When WG / responsible persons identifies all risks and control measures, responsible persons, etc. and before WG / responsible give the final product to superior for the approval and to sign, "final product" (risk register, integrity plan, action plan)) to all employees to inform them and to ask them about their opinion, proposals and suggestions.

For example, Annex No 7 to the Risk Assessment Guides of the beneficiary country is a good example of proper and efficient Action plan:

Risk Mapping Scale reference	Process Identification	Activity	Risk category	Detected Risk	Comments on detected risk	Action	Responsibility (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							
			Fraud							
			Corruption							

Step 6 – Implementation and Monitoring/review of CRM

CRM needs to be approved and signed by WG, Integrity manager and top management (superior) so that it becomes final and adopted product.

Implementation of CRM includes permanent:

- monitoring (recommendable every 3 months regards the implementation),
- periodical risk checks (controls) and
- updating of measures for elimination, reduction and monitoring risks (recommendable every year till the end of May).

Integrity manager (risk manager coordinator, etc.) should have in this phase crucial role:

- is a link between WG and superiors (head of institution) and employees,
- responsible for proposing solutions, aims, recommendations to superior,
- monitors and evaluates the timely implementation of measures,
- prepares report on implementation,
- responsible for up-dating CRM.

5. CONCLUSION

Mentioned steps are the most important phases and elements of Corruption Risk Management. Besides those, we would recommend to consider also following issues which helps CRM to be more efficient, clear and useful:

- Every action, decision by WG and Integrity Manager must be recorded (minutes),
- CRM must be mandatory tool, based on the law for all public entities,
- One guidelines for all institutions which should be obliged (by a law),
- Integrity manager must be a mandatory role inside the institution (also based on law),
- One central and independent body for supporting and monitoring CRM,
- Sanctions if CRM is not done in appropriate manner,
- IT solutions to help WG/responsible persons in the preparation and follow-up of CRM,
- Make the product user-friendly, simple and reasonable.

To conclude, handbook as prepared, shows that corruption risk assessment does not differ from the Risk Management system in the Beneficiary country and it only represents small (but very important) part of the methodology which is currently applied for risk assessment/management. Beneficiary country should “only” give more focus also on corruption risks.

Since the State Commission for the Prevention of Corruption of the Beneficiary country was according to the Law of the Prevention of Corruption established to implement the (international) measures and activities for prevention of corruption, it should represent a key partner in this process: to assist to institutions in identifying corruption indicators, identifying proper counter-measures on national (and perhaps on institutional) level regards corruption, preparing special (tailor-made) trainings for the most risk groups / institutions / persons, etc.