EUROPEAN
PARTNERS
AGAINST
CORRUPTION

INTEGRITY RISK MANAGEMENT

for

Anti-Corruption Authorities (ACAs)

and

Police Oversight Bodies (POBs)

GUIDELINE

Index:

Introduction

To fulfil their responsibilities, public bodies such as Anti-Corruption Authorities (ACAs) or Police Oversight Bodies (POBs) are increasingly using management tools which have so far mainly been applied in the private sector. These include project management, risk management or compliance management. In order to be able to benefit from these tools and make public administration more efficient, it is necessary to know the tools' methods, fields of application, added value and effects.

At the 16th Annual Professional Conference and General Assembly held from 15 to 17 November 2016 in Riga, the establishment of a working group on risk management and risk analysis was initiated. It started its activities at the beginning of 2017 and was chaired by Austria. The working group was composed of representatives from Austria, Azerbaijan, Bulgaria, Estonia, Germany, Hungary, Kosovo, Portugal, Moldova, Romania, Slovenia and Spain. Between April and September 2017 two WG meetings and an additional trilateral meeting were held in Austria, Slovenia and Moldova. Additionally, several written contributions have been considered.
At the 17th Annual Professional Conference and General Assembly from 15 to 17 November 2017 in Lisbon the guideline on integrity risk management for ACAs and POBs was presented and adopted as a working standard of and for EPAC/EACN member authorities.

This guideline aims to support EPAC/EACN members, both ACAs and POBs, in combating corruption and promoting compliance issues and to foster the development of a common risk policy among EPAC/EACN members.

The EPAC/EACN Working Group "Risk Management and Risk Analysis" proposes to present this guideline to the Council of Europe's Group of States against Corruption (GRECO) so that it could be applied in the framework of GRECO's 5th Evaluation Round.

1. General Perspective

Risk management is the professional approach to dealing with risks. It comprises all measures to identify, analyse, evaluate, monitor and control risks.

For Anti-Corruption Authorities (ACAs) and Police Oversight Bodies (POBs) risk management can be implemented in two ways, either by

- establishing a comprehensive risk management system to increase the effectiveness of ACAs and POBs themselves and to optimize the achievement of their objectives *(internal approach),* or by

- contributing to the performance of the task to be carried out by ACAs and POBs, i.e. the prevention of and fight against corruption, by identifying, analysing and evaluating corruption risks (*external approach*)

1.1 Internal and external risk management for ACAs and POBs

Especially in times of rapid change, organizations must quickly identify their risks and opportunities if they intend to protect, preserve and further develop their values. Risk management helps organizations to tackle this issue.

Due to their responsibilities, ACAs and POBs are often at the centre of public attention. They are obliged to carry out their tasks at the highest ethical level and in accordance with professional standards.
Risk management is a management tool aimed at identifying, analysing and evaluating the risks of an organization. For its implementation, it is necessary to define the organization's overarching goals, strategies, culture and policy regarding risk management.

This guideline shall serve as a basis for setting minimum standards on risk management in ACAs and POBs and for establishing risk management and risk analysis as tools facilitating corruption prevention work.

Internal risk management has a broader scope than the external one, as it may cover all kinds of risks for POBs and ACAs.
External assessment, on the other hand, provides organizations with more accurate and balanced information to assist them manage their integrity risks.

The methodology for internal and external assessment is rather similar. Both internal and external assessments have strengths and weaknesses when it comes to corruption and fraud management, in particular (please, refer to Annex).

1.2 Scope

This guideline

- contributes to raising awareness of anti-corruption matters (UNCAC, Art. 6)
- aims to establish minimum standards
- defines a common risk management policy according to the EPAC/EACN policy
- focuses on the practical use of risk management
- emphasizes the importance of risk management and risk analysis
- can be applied as a tool for corruption prevention and identifying integrity risks
- is designed for internal and external assessments
- shall be a basis for good management
- aims to protect against unlawful influence
- contributes to preventing conflicts of interests
- contributes to identifying risk levels and areas
- includes methods
- should be implemented as part of regular work, integrity plan, national, local or sectorial anti-corruption strategies and action plans

1.3 What is not intended

The objective of the working group or the guideline is not to merely describe standards, present national statistics, create a handbook, or to design a folder or flyer. It shall not be too complicated nor use ambiguous or unclear terms.

1.4 Target groups

- law enforcement bodies
- police authorities
- Anti-Corruption Authorities
- Police Oversight Bodies
- public bodies/departments

1.5 Preconditions

The following preconditions must be fulfilled:

- commitment of the management to implement an organizational culture of integrity
- commitment of the management to implement risk management (tone from the top)
- integration of the guideline into the national policy or other relevant policy
- resources must be available (budget, time and human resources)
- specific training must have been completed, certain skills must have been acquired

1.6 Training and skills

In order to be able to put into practice a well-functioning system of risk analysis and a management system, a solid basic knowledge of methods and the ability to practically apply these methods must be acquired.(see also chapter 6)

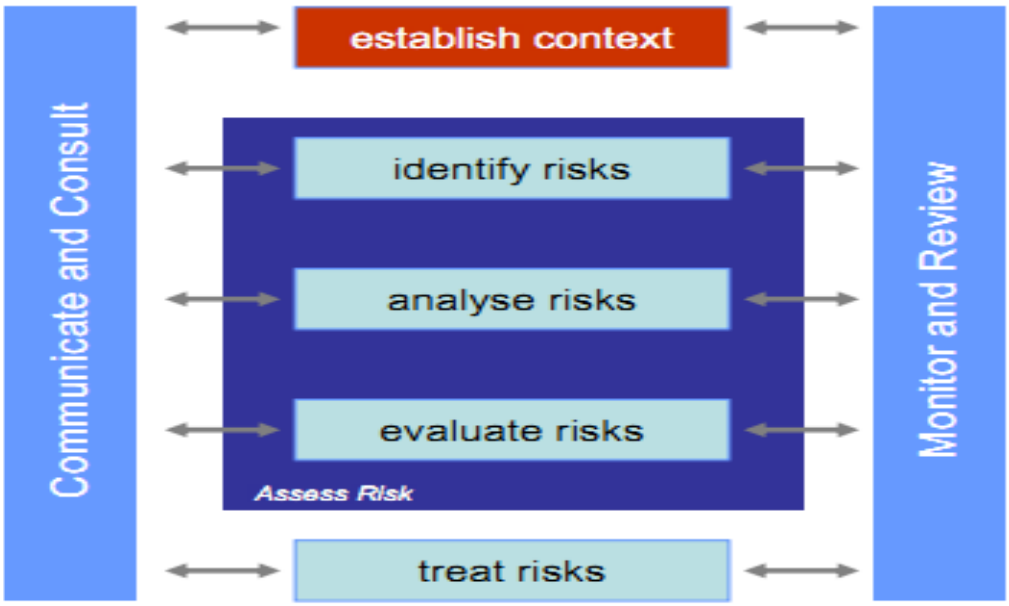
2. Key Elements for Integrity Risk Management

Following key elements are required to fulfill a necessary quality of integrity risk management.

2.1 Key elements

- all major working processes at all field of action
- legal assessments
- organizational culture
- human factors

2.2 Integrity risk management process:



Source: Victorian Managed Insurance Authority (VMIA), Risk Management by Stephen Owen (March 2010)

2.3 Integrity risk identification

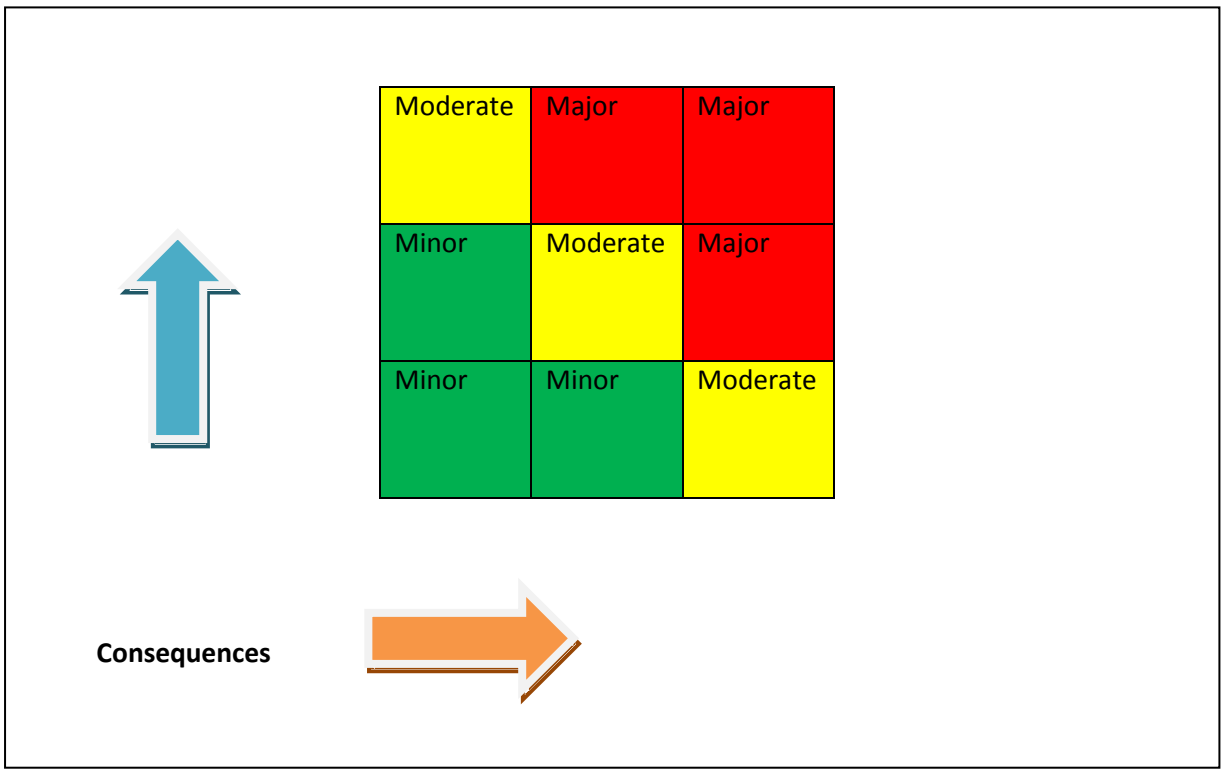
The integrity risk management process should always start with risk identification. For this, several methods are to be considered:

- creative methods, brainstorming, workshops
- methods of process analysis
- scenario analyses resp. (credible) worst case scenario
- law analyses
- case studies and root/cause methods (London Protocol, Ishikawa,….)
- best practice methods (see 5.4)
- webinars conducted by parties

(According to ISO 31000)

2.4 Integrity risk analysis and evaluation

When the integrity risks have been identified, they should be analysed and evaluated from the perspectives of likelihood and consequences. To facilitate this analysis, the use of a **minimum** 3 x 3 matrix is recommended:



Source: adapted version of the methodology described in the Integrity Plan of the Commission for the Prevention of Corruption, Republic of Slovenia

The following is an example of how to classify different levels of likelihood and consequences. This model can be adapted to the respective analysis and can also be used as a basis for 4 x 4, 5 x 5 etc. matrices:

Likelihood		
1	Very unlikely	once in 5 years, risk factor has never or – only once – occurred before
2	Likely (possible)	once in a year, risk factor could occur in the next five years; it may recur several times
3	Very likely (frequent)	once in 6 months, risk factor will occur in the next five years; it will recur several times

Consequences		
1	Minor	there are practically no consequences
2	Moderate	consequences are somewhat significant for the organization
3	Major (critical to catastrophic)	consequences are significant

Source: adapted version of the methodology described in the Integrity Plan of the Commission for the Prevention of Corruption, Republic of Slovenia

However, a sound risk management system requires tailor-made descriptions of likelihoods and consequences regarding the specificity of each organization.

2.5 Treatment of integrity risks

After the integrity risk identification and analysis, a decision should be made on the way of the treatment of the risk taking into consideration the risk tolerance level of the organization. This treatment strategy then needs to be included in an integrity plan. By way of implementing the integrity plan, the risk usually cannot be completely eliminated, only reduced under the risk tolerance level.

When choosing a risk treatment, the relation between the generic risk and the risk tolerance level should be taken into account as well as the fact that the risk treatment measures should be in balance with the possible consequence of the risk.

The most common ways of risk treatment are the followings:

Avoiding the risk: covers procedures aiming at the prevention of risks. Basically, it is the termination of an activity that may become a risk factor. It is easy to understand that this way can seldom be chosen by a public organization due to the fact that its activities are specified by law and not by individual decisions.

Devolving the risk: this means that the organization tries to find a partner that takes over the risk and also the responsibility of the risk treatment, usually for a reward. A

typical form is the outsourcing of a certain activity. As a downside, the secondary risks resulting from the outsourcing itself must be taken into account. This means that usually, outsourcing itself does not reduce the risk.

Risk mitigation: this is the most commonly used treatment that can be applied in relation to most of the risks. The central tool of risk mitigation is a plan (i.e. integrity plan) including the necessary measures to reduce the risk so that it remains under the risk tolerance level of the organization. This can either aim at reducing the likelihood of the risk or at preparing measures for reducing the consequences of the risk.

Retaining the risk: this term refers to consciously taking the risk. This can be a useful treatment in cases of relatively insignificant generic risks or where the expected effect of other ways of treating the risks would not be proportionate to the expenses. It is of course also possible that the organization is simply not in the position to treat the risk any other way than bearing it. However, such risks must be evaluated regularly and should not be forgotten.

2.6 Optional: monitoring and external audit

Additional monitoring and external audit procedures regarding the implementation of the risk management measures are recommended to increase and ensure their effectiveness and efficiency with measurable parameters/indicators.

3. Internal Risk Management for ACAs and POBs

In article 1.1 the importance of the implementation of risk management for internal use by ACAs and POBs is outlined.

ACAs and POBs can implement a risk management system with different kinds of assessments including

- analyses
- emergency and crisis management
- reporting and monitoring tools
- the establishment of a person responsible for coordinating risk management
- evaluation tools (Who monitors and how? E.g. supervisory bodies.)
- examination of the efficiency, goal-directedness, status of implementation etc. of the measures taken

These assessments can be used for all kinds of risks (compliance risks, safety and security risks, budgetary risks, etc.)

3.1 Tone from the top

Risk management must be considered as part of responsible leadership, i.e. as a management tool. Therefore, top executives should be able:

- to set an example living and explaining the "Tone from the Top" and the "Tone in the middle"
- to develop a risk policy with a certain strategy and culture
- to clearly define strategic objectives
- to make the organization stronger and the job environment safer
- raise awareness of positive opportunity management
- to use defined working processes as an educational tool for new employees

3.2 Integrity risks

Typical fields where integrity risks may arise are e.g.:

- procurement and property management
- conflicts of interest and favouritism
- giving and receiving gifts
- incompatibilities, restrictions and limitations
- post-employment restrictions
- undue/unlawful influences
- whistle-blower's protection
- human resources (recruitment, motivation, discipline)
- knowledge management – loss of know-how
- transparency and decision-making
- sponsoring
- operational field
- technology; access and storage of files
- IT & (personal) data protection and security
- financial irregularities
- intellectual property
- material and physical resources (misuse, loss...)
- instrumentalization of ACAs und POBs (unlawful influence)

3.3 Risk areas (legal perspective):

- laws/acts (e.g. offences of corruption and abuse of official authority, breach of official secrecy, illegal price agreements, money laundering, fraud, misappropriation/embezzlement, tax law etc.)
- organizational conditions
- work processes
- human factors

3.4 Additional risk areas if needed:

If required, the analyses can be extended to subfields with compliance and corruption risks in connection with strategic, operational, financial, socio-political or legal risks, or with environment or investment risks. They can also be applied in the context of buildings, fire protection, etc.

3.5 Implementation

How can risk management be implemented in your authority?

- Decide if risk management shall be implemented with a project team or within the hierarchy.
- Assign responsibilities and define a few steady rules of conduct.
- Inform all levels of …… (management, staff).
- Visualize the main working processes.
- Identify risks (workshops, documented proceedings, assessment from the reputational and the legal risks perspectives).
- Carry out a risk assessment.
- Register and analyse incidents and accidents in order to reassess the risks.

4. External Integrity Risk Management by ACAs and POBs

As outlined in article 1.1 above, external risk management is not a process happening entirely outside the organization facing integrity risks. It is rather an externally-driven integrity risk management, in which the external driving assessor is usually an ACA or a POB, while the assessed organization has to treat the risks identified, analysed and evaluated by the assessor. External integrity risk management represents rather a corruption prevention tool employed usually by the ACAs and POBs in carrying out their mandate.

As the methodology for internal and external integrity risk management is similar, the articles bellow will only illustrate the peculiarities of the external assessment as compared to chapter 2 of this guideline.

4.1 Selection of organization

The first difficulty in conducting external corruption risk assessment is to prioritize and focus on public organizations particularly vulnerable to corruption.

Criteria to select an organization for external integrity risk management could be:

- statistics on perceived or investigated levels of corruption
- vulnerability of activities carried out
- exposure to direct contact with beneficiaries of public services
- insufficient implementation of national and sectorial anti-corruption policies

4.2 Sources for integrity risks identification

It is very important to rely on objective sources of information in the process of identification of integrity risks within another organization. In addition to the methods described in article 2.3, additional sources might be:

- information on past integrity incidents
- complaints from citizens and other intelligence held by ACAs and POBs;
- analytical reports, surveys, assessments, workshops etc. on corruption in the organization
- conclusions of audits and inspections conducted by superior and oversight bodies
- workshop findings
- media coverage

4.3 Corruption risk factors

In analysing the factors of (factors which determine) the emergence of corruption risks, the ACAs must pay particular attention to:

- external risk factors
- internal risk factors
- operational risk factors
- individual risk factors

4.4 Publicity

Unlike the internal risk management for ACAs and POBs, which may encompass a broader area of risks which are not to be disclosed to the general public, the external integrity risk management should strive to be transparent. It would be important to make anti-corruption, anti-fraud and integrity-promoting efforts visible to the public.

A motivator for an organization to change in that respect could be the acknowledgement of its corruption issues and a public commitment to grow an integrity climate. However, it depends on each country's legal framework whether this approach can be implemented or not.

4.5 Application in anti-corruption and integrity education

The tool can be used for preventive activities such as information events, seminars, training courses, coaching and workshops or for drawing up lists of dangers, for the identification of risks, or risk analysis with assessment, and whenever there is a specific need and the necessary resources are available.

A risk analysis carried out and documented within the framework of a workshop aims to identify the reasons for the risks, their consequences and the likelihood of their occurrence. The deliberate focus is on compliance risks, i.e. on human and organizational reasons.

5. Minimum Requirements for Risk Managers / Integrity Advisers

Risk managers should be embedded in the organizational structure, and processes are necessary which allow for continuous follow-up of risks.

5.1 Skills

Risk managers must have knowledge of the following instruments of compliance management:

- development and implementation of codes of conduct/behaviour guidelines
- measures to increase integrity
- communication and training methods (methodology & didactics)
- establishment of a compliance management system
- instruments to implement a culture of integrity
- in cases of emergency: crisis management and business continuity management
  e.g.
  - communication with public bodies, audit authorities, internal audit departments, auditors, public prosecutor's offices and courts
  - professional case handling

5.2 Further training

The compliance and risk manager is obliged to regularly undergo further specialist training so that his/her qualification corresponds to the current state of technology and legislation.

5.3 Learning outcomes and acquisition of skills

- Identifying, analysing, assessing, illustrating and documenting risks within different fields, systems or departments of several ministries.
- communicating the benefits and added value of a risk analysis and a risk management system to senior officials
- using practice-oriented tools to identify and assess risks
- applying tools of risk and hazard analysis correctly
- mastering methods of risk analysis
- understanding and applying error handling as well as tools of accident and cause analysis (London Protocol, CIRS, Ishikawa)
- contributing substantially to the improvement of transparency in the respective company/authority through forward-looking risk management throughout the organization

5.4 Methods for the training of risk managers

- basic knowledge acquired through reading and studying in advance
- keynote speeches
- exercises and interaction within workshops
- behaviour training (for specific situations)
- best practices, methods and case studies
- discussion and reflection

6. Basic terms

(1) **Risk:** is the effect of uncertainty on objectives. An effect is a positive or negative deviation from what is expected.

(2) **Risk owner:** is a person or entity that has been given the authority to manage a particular risk and is accountable for doing so.

(3) **Risk assessment:** is a process that is, in turn, made up of three processes: risk identification, risk analysis, and risk evaluation.

(4) **Risk identification:** is a process that involves finding, recognizing, and describing the risks that could affect the achievement of an organization's objectives. It is used to identify possible sources of risk in addition to the events and circumstances that could affect the achievement of objectives. It also includes the identification of possible causes and potential consequences. Result: list of dangers, inventory of risks.

(5) **Risk analysis:** is a process that is used to understand the nature, sources, and causes of the risks that you have identified and to estimate the level of risk. It is also used to study impacts and consequences and to examine the controls that currently exist. The results will be transferred to a matrix.

(6) **Risk evaluation:** is a process that is used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable or tolerable and which risks will be tackled first.

(7) **Risk factor:** is the cause of the risk. Usually they are elements that generate risks in the future. Simultaneous occurrence of more than one risk factor can increase either the likelihood or the consequence of the risk or both.

(8) **Risk tolerance level:** is the level of exposure to risks of the organization above which countermeasures shall be applied. It should be determined by the manager of the organization and is influenced by organizational culture, availability of sources and technical possibilities.

(9) **Integrity plan:** is a document approved by the manager of the organization that aims at the treatment of the integrity risks. An integrity plan should contain at least: measures to treat the integrity risks, deadlines, responsibility for implementation and progress indicators. For an integrity plan to be successful, the management's commitment, accountability in implementation, an impartial monitoring and oversight are required

(10) **Risk treatment:** is a risk modification process. You have many treatment options. You can avoid the risk, remove the source of the risk, modify the consequences, change the probabilities, or you can simply retain the risk.

(11) **Risk monitoring:** aims to ensure the correct implementation of the risk treatment measures; continuous or periodic monitoring.

(12) **London Protocol:** scenario methods to analyse damage events that have already occurred, used in order to identify risks and their causes.

(13) **Risk management system:** systematic application of management principles and processes to communicate, identify, analyse, evaluate, treat, monitor and control risks. It is not an independent element but an integral part of all organizational processes. It helps decision-makers to act on the basis of information, to prioritize measures and to choose from various possible solutions.

7. Sources

- Adapted version of the methodology described in the Integrity Plan of the Commission for the Prevention of Corruption, Republic of Slovenia
- Austrian standard ONR 192050:2013 „Compliance Management Systems (CMS) – Requirements and Application Guideline"
- Austrian standard ONR 49000-49003:2014 „Risk Management for Organizations and Systems – Terms and Principles"
- Corruption Risks Assessment in Public Institutions in South East Europe. Comparative Research and Methodology prepared for the Regional Anti-corruption Initiative (RAI) 2015.
- ISO 31000:2009 "Risk Management"
- ISO 37001:2016 - "Anti-bribery management systems"
- Methodological guide for the development of control environment and the integrated risk management system – National Protective Service, Hungary
- United Nations Convention against Corruption (UNCAC)
- Victorian Managed Insurance Authority (VMIA), Risk Management by Stephen Owen (March 2010)

Annex:

Strengths and Weaknesses of Internal and External Assessment

Assessment type	Strengths	Weaknesses
Internal (self) assessment	- tailored assessment process based on 'insider' knowledge of internal environment and working processes - learning and development process - can help develop confidence of public officials in what they are doing well, - conducted with internal resources	- danger of being merely a check-list or of poor quality - possible absence of sufficient commitment of superior and/or staff, - lack of sufficient knowledge or/and experience for implementation of assessment, - time-consuming
External assessment	- potentially broader scope of assessment - expert knowledge and experiences in assessment methodology - independent and objective assessment - less time consuming for the subject under assessment	- less in-depth assessment, - more robust assessment process, - possible concealment of certain internal particularities or vulnerabilities from external evaluators, - superficial or insufficient knowledge of working processes in institution, sector or project under assessment -

Source: "Corruption Risks Assessment in Public Institutions in South East Europe". Comparative Research and Methodology prepared for the Regional Anti-corruption Initiative (RAI) / 2015.