**FWC SIEA 2018 – EuropeAid/132633/C/SER/Multi**
**Lot 3: "Human Rights , Democracy and Peace"**
**Contract n° 2019/414393**

# "TECHNICAL ASSISTANCE TO THE NATIONAL COORDINATOR AGAINST CORRUPTION SECTOR REFORM CONTRACT FOR THE FIGHT AGAINST CORRUPTION

## Integrity Risk Assessment Manual

*October 2021*

*Activity 2.f.3*

Project financed by the European Union

Project realized by ARS Progetti S.P.A.

A.R.S. Progetti S.P.A.
Ambiente Risorse Sviluppo

This report has been prepared with the financial assistance of the European Commission. The views expressed herein are those of the consultants and therefore in no way reflect the official opinion of the Commission.

# Table of Contents

## 1. INTRODUCTION

Under the national Inter-Sectoral Anti-Corruption Strategy and its Action Plan all Albanian public institutions must elaborate Integrity Plans, defining measures they will implement to prevent and tackle breaches of integrity by their personnel that occur or are likely to occur. In order to elaborate such Plans, each institution must first conduct an Integrity Risk Assessment. An Integrity Risk Assessment (IRA) Methodology for conducting such assessments exists for Central Government Institutions, approved by the Ministry of Justice (MoJ) in November 2020.

IRA is a self-assessment implemented by the organization itself. The aim of the Guide is to provide a framework for both management and the Integrity Coordinator. Management can use this guide as a starting point for implementation and the Integrity Coordinator can use it for the concrete structuring and processing of the risk assessment.

This Guide follows the 5 stages of the risk assessment. The method presented is constructed in such a way that the members of the IRA Working Group are supported with practical material at each stage of implementation of the assessment. Background information and examples are provided in Section 3. If the Guide is primarily a web resource, additional examples could and should be added online to enable users to learn from a range of real-life examples as possible.

The Guide does not aim to provide an exact "blueprint risk assessment" that can be cut and pasted in any institution. It rather provides tools so that officials responsible for IRA can more easily design assessment IRA tailored to the needs of their institution. On request of the Ministry of Justice, the Guide has been kept as brief and concise as possible.

### What this guide provides and for whom?

Integrity Risk Assessment has a primarily *preventive character* and is **not** focused on the detection of corrupt persons or investigation of specific integrity breaches. This guide therefore provides a roadmap to enable officials responsible for risk assessment identify and assess risks and risk factors, so that they can elaborate an Integrity Plan whose main objective is to address those risk factors.

This Guide is provided for central government institutions. However, two important points should be noted. First, the methods of assessment are of equal relevance to any public entity, including local government.

Second, it is essential to be clear which exactly are the entities that conduct risk assessment. In Albania each ministry and other central institutions (such as Agencies) has to draft its own Integrity Plan (and therefore conduct their own IRA). Institutions that are subordinate to them also have to conduct their own IRAs. It is essential that after each institution has done this the outputs of assessments and integrity plans that relate to the same government functions are brought together in some way so that they are coordinated.

## 2. STAGES OF THE RISK ASSESSMENT

The Risk Assessment should be conducted in the following stages:

Stage 1: Set-up of a team/Working Group and describe its tasks.

Stage 2: Identify areas of the institution's operation on which the IRA will focus - vulnerable processes and vulnerable positions.

Stage 3: Within the areas the IRA focuses on, identify integrity risks and the risk factors that make those risks more likely to occur.

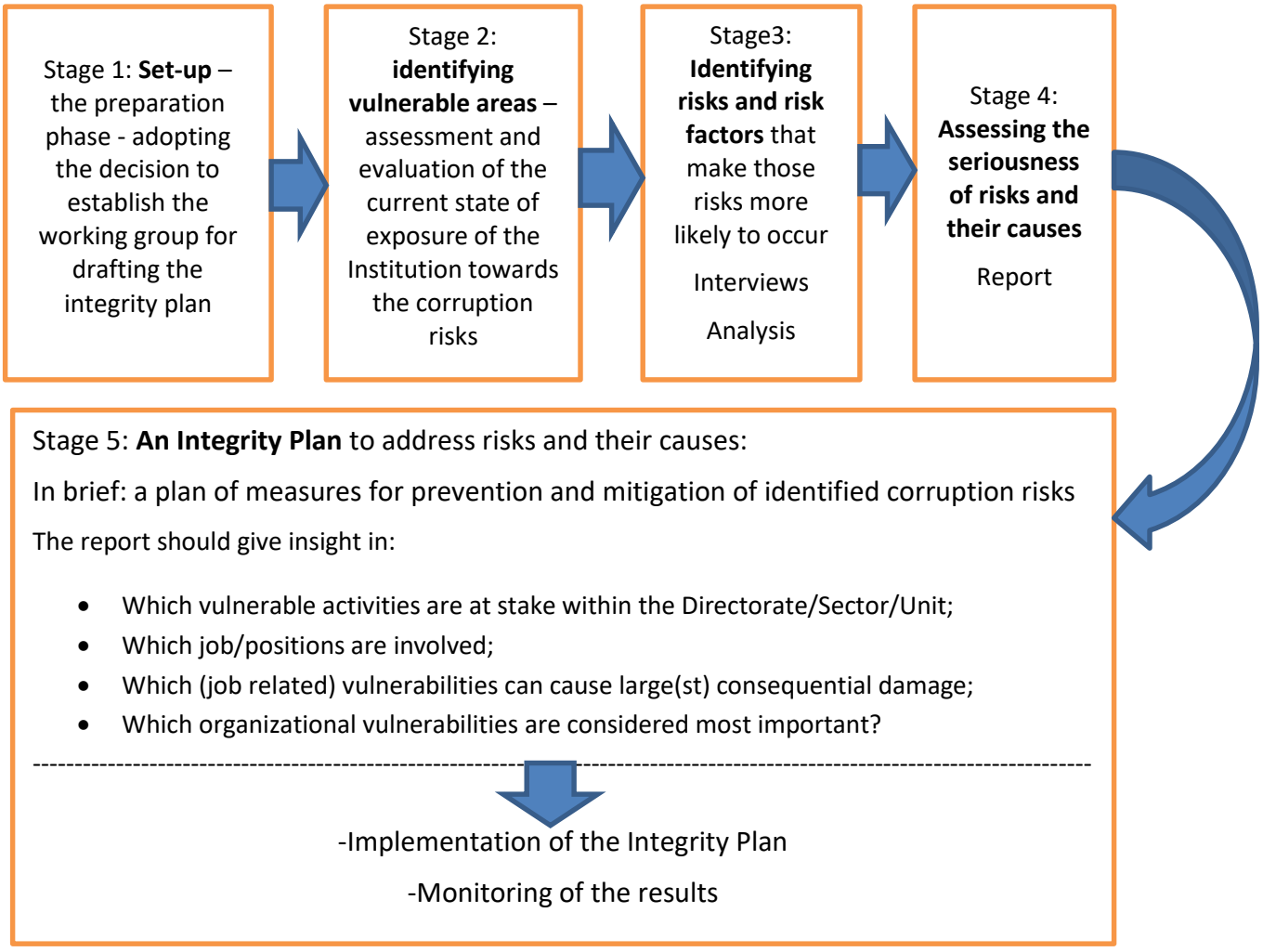
Stage 4: Assess the seriousness of the risks and risk factors.

Stage 5: Draft an Integrity Plan - measures to address risk factors (causes/reasons why risks are present or serious) and to address the risks themselves (mitigation)

These stages are explained in more detail below.

An additional stage of the IRA cycle is monitoring and reporting on Integrity Plan implementation. This Guide focuses on the design and implementation of the IRA itself.

## Stages of Integrity Plan/Risk Assessment development:




**Stage 1: Set-up**: At this stage a team (Working Group) is selected to conduct the IRA. The head of the institution or a highly ranked official (the Integrity Coordinator is the obvious candidate) must take part at this stage and officially authorise the Working Group and its remit, to ensure high-level commitment and clearly delegate authority to the group to actually conduct the risk assessment. The team should have the authority to interview anyone in the institution that is deemed necessary, and persons so selected must be obliged to cooperate.

A key requirement for the team is that it must bring together persons with different expertise to bring together for example analysis of legal acts, interviewing of officials and other stakeholders, elaboration

of measures to address causes of risks, etc. A risk assessment will usually need a multidisciplinary team to be conducted well.

**Stage 2: Identifying vulnerable areas**

A risk assessment does not – and almost always should not – try to examine every area and process within an institution, especially a large institution. Resources (primarily people and time) are always limited and important risks will generally be concentrated in certain key areas or processes – or **vulnerable areas**. To focus resources effectively, **risk assessment should focus on areas of the institution's activity (functions/processes) that are naturally vulnerable to integrity breaches**. For example, under the remit of the General Directorate of Prisons vulnerable areas might include regulation and management of the following: visits to prisoners (family life), evaluation of prisoners' conduct, determination of prisoner incentives and privileges, managing prisoners' property, use of segregation and/or solitary confinement, sentences and parole, use of force, proceedings against prisoners, and complaints mechanisms for prisoners and staff.

Once functions/processes have been selected, the Methodology of the MoJ lists five areas that should be covered in all institutions:

- Financial Management
- HR Management
- Control, audit and AC mechanisms
- Transparency
- Archiving, storing and administering of documents as well as information, and electronic documents

**These five common areas should be understood as areas of management that are important in all activities of the institution**. They should be examined in two different ways. First, where appropriate, general provisions relating to each area should be examined – for example rules of financial management or on recruitment that apply to the whole institution, or on dealing with requests for information. Second, they should be scrutinised specifically within each vulnerable area selected. For example, general rules on access to information will apply to an entire ministry. However, in the area of procurement within the ministry, specific issues of transparency will need to be examined – for example rules on the publication of contracts, losing bidders etc.

Vulnerable areas may be identified by organising one or two meetings of key stakeholders, meaning:

- The Risk Assessment Working Group (team)
- Heads of Departments (or equivalent organisational units within the institution)
- A broader range of employees of the institution
- Other important stakeholders, such as clients (those using services provided by the institution), external experts etc.

**Identifying vulnerable processes and positions**

Vulnerable areas may be understood as vulnerable processes, within which certain positions within them (occupied by officials) may be identified as specifically vulnerable.

**Vulnerable positions** may be defined essentially as positions whose occupants control resources that provide an incentive to engage in integrity breaches, or be a target for external parties with an interest in inducing the official to engage in integrity breaches. Resources may be divided into the following types, for example:

- Financial resources (money, cash)
- Assets
- Regulatory resources, e.g. permissions/permits that grant access to economic resources

- Human resources (positions)
- Information/data
- Control/oversight resources, e.g. audits, inspections etc.
- Contacts within or outside the institution

Examples of vulnerable positions would include for example a budget director, financial controller, official issuing permits, member of housing allocation commission, head of investment department, etc.

**Stage 3: Identifying risks and risk factors**

**Integrity risks**

Integrity risks are actual breaches that occur or are likely to occur in an institution or process. The more likely a particular breach of integrity risk is to occur, and the greater the damage caused by it if it does occur, the more severe is the integrity risk. Examples of integrity risks include:

- Corruption: accepting/requesting bribes, providing/offering bribes, trading in influence, embezzlement, nepotism, cronyism (advancing interests of other kinds of associate such as friends, business associates), and other abuses of position for personal interest – for example where a doctor wrongly refers a patient to a specialist clinic where the doctor operates privately. It also may include actions that advance the interests of other entities such as performing party political tasks during working hours.
- Performing tasks incompetently or lazily (poor quality of work outputs, inefficient/slow work, failure to perform tasks),
- Treating citizens/clients unequally (e.g. discriminating) or unfairly (e.g. being rude/abusive)
- Failure to follow legal procedures/requirements, irrespective of whether decisions are correct ones or not.
- Obstructionism/formalism – for example "working to rule", where officials do only what is the minimum formally required of them.

**Integrity risk factors**

These are the factors that make integrity risks more likely to occur – they may be characterised roughly as "causes of" or "reasons for" integrity risks. Examples include the following

- Legal acts/procedures that
    - Give officials excessive discretion in making certain decisions (for example to award contracts, select recipients of social housing, impose sanctions for breaches of rules, etc.)
    - Do not include well-designed mechanisms for holding officials responsible for their decisions
    - Fail to ensure sufficient transparency of decision-making and decisions.

  Note: Section 3.3 on "Corruption proofing" of legal acts, as well the Section below on the "Analysis of legal and regulatory documents" elaborates on these risk factors in more detail.
- Problems in management of human resources, including for example
    - Failure to recruit permanent staff to vacant positions, use of temporary contracts etc.; note that this might also be seen as an example of an integrity breach depending on the context and details.
    - High turnover of staff.
    - Poor working conditions including pay, physical environment (offices, equipment etc.), and other factors.

    - Lack of job descriptions
    - Absent/inadequate training
    - Demoralised staff.
- Gaps or problems in framework and mechanisms for ensuring integrity, for example:
    - Absent/inadequate conflict of interest rules
    - No code of conduct/ethics
    - No/inadequate training/awareness raising on integrity framework
    - Procedures not in place or implemented for protecting whistle-blowers
    - Failure to properly implement framework for asset declarations

**What are we trying to find out?**

The type of information we need to find out may be divided into four main areas: formal rules governing processes, working conditions, the integrity framework in place, and the implementation of processes in practice.

**Formal rules governing process/es**

The main question here is whether the process/es on which we are focusing are clearly described in rules, and set up in a way as that the rules do not unnecessarily facilitate or encourage integrity breaches. This may be assessed by screening the rules using the corruption proofing methodology provided in Section 3.3.

**Integrity framework**

The IRA should gather information on what specific rules and frameworks are in place to set appropriate standards of official conduct, help officials to observe the standards and enforce compliance with them where appropriate. This may be done by asking the same questions that comprise Section IV of the MoJ questionnaire, but rephrased so that they are about the framework itself, not about employees‘ awareness or perception of it.

**Implementation of process in practice**

The IRA should assess which integrity breaches occur are likely to occur during the implementation of the process/es under scrutiny – in other words, which integrity risks are present. For this, Section 3 of the MoJ Questionnaire may be used along with questions 40 (application of conflict of interest rules in practice), 42 (whether promotion is based on meritocracy), 44 (internal communication rules), and 46 (dealing with confidential information).

**Working conditions**

The question to be addressed here is whether officials who are responsible for the implementation/administration of the process/es have the conditions that are necessary for them to be able to perform their work impartially and effectively. For this purpose, a survey of employees using the questionnaire provided in the Ministry of Justice IRA Methodology can provide much of the information needed (or the questionnaire may be used as a basis (source of questions) for interviewing officials).

In addition to the structured questions contained in the questionnaire, a more open-ended question should be asked to the officials interviewed, namely: “Are they satisfied with their job and working conditions – and if not why not”? Such a question may reveal problems that constitute significant or even serious integrity risks yet are not always “caught” by a formal integrity risk assessment. One interlocutor in Albania noted that demoralisation of the staff of his/her unit; this itself may a serious integrity risk factor, even if it does not fall under the standard headings such as procedural integrity, accountability and transparency.

**Sources of information**

The IRA Methodology lists three main methods for gathering information: analysing legal acts, official and other documents; conducting interviews with persons within the institution/process and/or from outside it; and conducting formal surveys – usually of employees of the institution but potentially also of other stakeholders such as service users.

**Interviews**

Interviews are in practice usually the most important method used in a risk assessment. They aim to gather information of a descriptive nature – for example answering questions of the following nature, reflecting the sample questionnaire provided above:

- How does this process work in practice?
- What forms of poor conduct (integrity breach) take place or are likely to take place during its implementation?
- What aspects of the process (its design, the rules, institutional set-up for implementation, etc.) make such integrity breaches more likely?

Interviews should be conducted firstly with the employees of the institution who are most likely to know the answers to the questions you are attempting to answer. Where possible, interviews should also be conducted outside the institution.

**Surveys**

Surveys are a way of gathering information on the opinions, perceptions and/or experience of participants in a way that can in principle of measured and used statistically. The MoJ Methodology includes a sample questionnaire that can be used as a basis to gauge the awareness, perceptions and to some extent experience of employees of the institution However, if a survey is conducted then the questionnaire will need to be tailored to the needs of the specific institution. In practice surveys will probably be used less often than interviews and documentary analysis.

**Analysis of legal and regulatory documents**

A central component of risk assessment is screening of the legal framework that governs the institution or process that is being assessed. This means primary laws, by-laws (sub-legal acts) and any other binding rules and regulations. It should also include documents that are not strictly legally binding, such as guidelines, manuals etc.

The aim when analysing legal and regulatory documents is to screen them for provisions that increase the risk of integrity breaches will occur. Such screening is known as “corruption proofing”, and methodologies are readily available for implementing it. The criteria that should be used for screening are provided in Section 3.3.

**Other and non-official documents**

In addition to legal acts and other rule-determining documents, other official documents may be valuable source of information for identifying risks and/or risk factors. These include reports of inspections, controls, audits. They would also include any other analytical/policy documents that have been elaborated. Documents may be internal (for example inspections) or external (for example High State Audit reports).

Often, documents produced by external entities may be useful as a source of information on the functioning of your institution and its processes. These will be for example NGO reports, analyses (e.g. monitoring), and similar media reports on the activities of the institution.

For both official and non-official documents, these should be scrutinised to determine whether they identify integrity risks or risk factors in the processes of your institution that you are focusing on.

**How to analyse government functions and processes**

For each government function/process assessed under the IRA, a challenge is how to analyse and assess it practically. To do this, divide the function/process into its constituent parts. A good example of this is public procurement, which may be divided for example into six logical phases: determining needs, preparing selection phase, selection, contracting, contract implementation, accounting and auditing. Annex 4 of the MoJ Methodology provides this example in more detail, listing issues that might be focused on under each phase, relevant indicators of procurement performance, and sources of information.

**Describing risks: be specific!**

Stage 3 defined risks in general terms as integrity breaches, and provided some examples. However, these are quite general examples. When describing risks in a specific process or institution, it is essential to be as specific as possible, because knowing the exact nature of an integrity breach makes it easier to identify the reasons/causes (risk factors) – and therefore which, measures are needed in the Integrity Plan. For example, in the example of public procurement a risk as general as "bribery in the awarding of tenders" should not be cited. The description could be for example "Solicitation by procurement commission members of payments from executives of companies competing in tenders in return for favouring the companies unjustifiably in tender proceedings."

**Stage 4: Assessing the seriousness of risks and their causes**

The IRA should yield a list of risks, i.e. integrity breaches that are through to occur or be at risk of occurring in the institution. Once risks are identified in this way, you should make an assessment for each risk of the following:

- **Probability**: how likely is this integrity breach to occur? For practical purposes, assess whether the probability of a risk occurring is low, medium or high.

- **Impact**: if the integrity breach does occur, what is its likely impact – in other words, what damage is it likely to cause. Key types of damage are financial (loss of funds/assets), poor decision-making with the impacts that has on subjects of decision-making, impact on reputation and trust in the institution or its processes. The severity of impact may also be classified as low, medium or high in all of these areas.

- **Overall risk severity**. The combination of probability of a risk occurring and the impact if it does occur can be used to make an assessment of the seriousness of the risk. This may be done roughly example by assigning scores of 1, 2 and 3 to "low", "medium" and "high" and then multiplying the figures for probability and impact for each risk. For example, a risk that was low in probability and low in seriousness would score 1 overall, but one that is high in probability and also high in impact (severity) would score 9. This should not be assumed to be an exact measure of risk severity, just a rough indicator.

**Assessing the importance of risk factors**

For each risk (integrity breach) identified, the IRA will have identified risk factors that facilitate the risk or make it more likely to occur. For example, the provision of confidential personal data to outside entities may be a risk, and one of the risk factors facilitating this may be lax control or monitoring of access to IT systems. The more serious is a risk that has been identified, the more importance should be attached to the risk factors underlying it. In the example, if the provision of confidential data to outside entities is assessed as a high risk, lax control of access to IT systems would (other things equal) be likely to be seen as an important risk factor – and therefore one that should be allocated priority in the Integrity Plan that is drafted on the basis of the Risk Assessment. Clearly, not all risk factors will be of equal importance for a given risk: the relative importance of each risk factor cannot just be derived from simple risk scores and must be judged in context.

**Stage 5: An Integrity Plan to address risks and their causes**

The Integrity Risk Assessment should have yielded the following:

- A list of integrity risks – i.e. integrity breaches that have occurred, occur or are assessed as being likely to occur, classified according to their severity
- A list of integrity risk factors – i.e. the factors/aspect of the legal, institutional or operational framework that make the identified risks (breaches) more likely to occur

Once the integrity risks and risk factors are identified, the IRA should be use to draft measures to address the integrity risks and risk factors. The measures drafted constitute the institution (or relevant entity)'s Integrity Plan. Measures are of two types:

- **Preventive measures**. These are measures aimed at addressing the risk factors, i.e. the causes or factors facilitating integrity breaches (risks).
- **Mitigation measures**. These are measures designed to address risks (.e. integrity breaches) that actually occur.

**Examples of preventive measures** would be:

- Implement hiring procedures (and ensure sufficient resources) to minimise the number of temporary contracts to a necessary minimum and ensure positions in the organigram of an institution are fully occupied.
- Clarifying a procedure to ensure that
  - Responsibilities of officials do not enjoy unnecessarily wide discretion in the decisions they make to implement their responsibilities;
  - Job descriptions are in place;
  - Etc.
- Pass or modify/improve a code of conduct.
- Ensure regular high-quality training on standards of conduct.

**Examples of mitigation measures** include:

- Strengthening internal inspections of official activities.
- Increasing (disciplinary) sanctions for integrity violations.
- Launch an investigation into a specific case or area of wrongdoing that the IRA happened to reveal.
- Etc.

Again, it is important to stress that the primary objective of an Integrity Plan should be to define measures that lower the incidence of integrity breaches – in other words, preventive measures.

## 3. BACKGROUND INFORMATION AND EXAMPLES

### 3.1 Key concepts

**Integrity**

For practical purposes, integrity means being diligent (i.e. performing one's duties to the best of one's ability), taking responsibility for one's conduct (i.e. being accountable), treating others fairly and conducting oneself honestly.

**Integrity breach**

An integrity breach occurs when an individual acts in a way that is not in accordance with the standard of behaviour defined above. Integrity breaches include corruption (for example taking money in return for providing a citizen or client with a benefit), but also include acting incompetently or lazily, treating people unequally/unfairly, or any conduct that undermines the impartial and effective performance of public (government) functions (such as the provision of public services).

**Public service function**: the public services or tasks an institution and its processes are supposed to deliver/perform.

**Risk**: a specific form of integrity breach that might occur. For example, in a public procurement process, many possible types of poor conduct may occur, such as: procurement officials taking a bribe from a tender participant in order to award them the tender; procurement managers designing tender conditions so that only one company can win it; exempting a procurement process from the requirement to hold an open tender; allowing entities that do not fulfil requirements for tender participation to bid; collusion between bidders to ensure that one wins; drafting contracts that diverge from the tender conditions/winning bid; failure to supervise contract fulfilment; etc.

**Risk factor**: an aspect of the legal, institutional or practical set-up of an institution or one of its processes that makes it more likely those risks (i.e. integrity breaches) will occur. The examples of poor conduct above – "integrity breaches" – will often be facilitated by problems in the legal or institutional framework. For example, integrity breaches in the procurement process may be enabled by unclear rules for budget planning and determining investment needs, inadequate provisions to prevent conflicts of interest of persons responsible for procurement, tender rules that enable the provision of too many contracts without competition, weak or absent rules governing the drafting of contracts following a contract award, lack of mechanisms to ensure monitoring of contract fulfilment and costs, etc.

**Integrity Risk Assessment**: the assessment of the likelihood and seriousness of risks (integrity breaches) in an institution or process, and identification of the risk factors that make those risks more likely to be realised.

**Integrity Plan**: A plan of measures to address risks through i) PREVENTIVE MEASURES: addressing the risk factors that underlie or facilitate them, and if necessary ii) CONTINGENCY MEASURES: measures to deal with risks (breaches) that do occur. The prime focus of an Integrity Plan should normally be on preventive measure – addressing the causes not the consequences.

### 3.2 The range of integrity risks

A corruption/integrity risk assessment conducted in 2017 by the city administration of Sabadell, a town of 200,000 people in Spain identified seventy-four integrity risks, including the following:

- For one's own interest or those of third parties, and without objective justification:
    - Altering a file
    - Modifying the meaning of a report
    - Altering the order of official actions
    - Giving priority to certain files or actions
    - Failing to initiate, resolve or leaving to expire files
    - Applying regulations in a different way in equivalent situations
    - Manipulating registration and waiting lists
    - Providing inside information to specific applicants in selection, procurement or promotion
    - Prioritize the approval and payment of invoices of certain individuals
    - Provide protected personal data to companies or individuals
    - Accessing digital personal data

- Drafting criteria for personnel selection to suit particular candidates
- Favouring specific candidates in staff selection interviews
- Making non-urgent interim appointments to circumvent selection processes
- Unjustified absence during working hours due to private professional tasks
- Absence during working hours due to personal issues
- Engaging in more lax mutual control due to personal affinity
- Adapt/tailored procurement specifications to specific commercial interests
- Dividing contracts to avoid contracting processes.
- Accepting from natural or legal persons favours that influence decision-making
- Accepting gifts or invitations from third parties
- Using the Administration for exclusively partisan interests
- Failure to impose sanctions
- Not recording negative findings in an inspection
- Misuse of transportation tickets or municipal vehicles
- Advise the granting of a subsidy to some entities
- Use credit cards for private use
- Failure to comply with the duty of confidentiality of information
- Consult personal data for reasons other than work
- Provide non-public information on grants to certain entities or individuals
- Allow private use of municipal facilities on behalf of an entity

### 3.3 Criteria for screening legal and regulatory acts/documents for integrity risk factors

Provisions of legal and regulatory documents should be screened to check if there are any provisions that increase the risk of officials engaging in corruption or other integrity breaches. Problematic provisions may be divided into three main categories:

1. Provisions that create conditions in which officials enjoy excessive discretion due to:
    a. Unclear, ambiguous or inconsistent terminology (e.g. using a term to mean different things in different parts of the law, using different terms for the same thing, etc.).
    b. Failure to establish criteria or clear criteria for official decisions – thereby enabling officials to make decisions arbitrarily.
    c. Legal provisions that conflict with each other – enabling officials to choose which provisions to use/comply with. E.g. (e.g. criteria for receiving a service are different in a main law than in its implementing regulations)
    d. Faulty reference provisions, meaning provisions that do not make clear enough references to other provisions in the same legal act or other legal acts.
    e. Provisions that leave to be defined in secondary legislation (decrees, etc.) important rules that should be defined in the primary legal act.

2. Provisions that do not establish adequate mechanisms to ensure the accountability of officials and institutions for decisions. This may be due to:
    a. Failure to designate or designate clearly the persons or entities responsible for decisions or other actions related by the law.
    b. Failure to establish adequate mechanisms for appeal and redress against decisions.
    c. Failure to establish adequate mechanisms for complaints against the conduct of officials or institutions.
    d. Failure to establish adequate sanctions applicable to officials or institutions that fail to fulfil their legal obligations.
    e. Failure to establish adequate sanctions applicable to other entities regulated by the law for failure to fulfil their legal obligations.

3. Provisions that do not require sufficient transparency relating to decisions or actions regulated by the legal act:
    a. Insufficient or absent requirements to publicise/disseminate information on procedures, rights and obligations established or regulated by the act.
    b. Absent/insufficient requirements to inform interested/affected parties of decisions affecting them.
    c. Absent/insufficient requirements for publication of decisions/actions regulated by the legal act.

### 3.4 Example from the Albanian Ministry of Justice: General Directorate of Prisons, 2021

Each of the vulnerable areas of an institution selected for assessment should be divided up into their constituent parts. For example, complaints mechanisms in prisons could be divided up into the following components: definition of complaint, types of complaint/issues on which complaints may be filed, accessibility (who may submit complaints), format of complaints, process for filing complaints (verbal, in writing, anonymous permitted?, entry points/means for submitting etc.), rules for processing complaints (who reviews complaints – internal/external etc., what are the deadlines, under what circumstances are complaints leading to an investigation/forwarding to higher authority etc.).[1]

Another example - from the General Directorate of Prisons - is the procedure for evaluation of prisoner conduct. A workshop conducted in June 2021 included discussion of the process of evaluation. The process was deemed vulnerable because the results of evaluation can have important impacts on prisoner welfare, both within prison (access to privileges etc.) and outside (by possibly influencing parole/release decisions. In order to actually assess the framework for evaluation, the brief discussion yielded the following possible questions, although these may not be complete:

- Which are the criteria for evaluating prisoner behaviour?
    - Are they clearly defined and understandable for those conducting evaluation and for prisoners themselves?
    - Are they measurable where possible?
    - Are they reasonable and fair?
- Are there clear rules and procedures on whose input is gathered for evaluation?
    - Staff?
    - Prisoner?
        - Formally interviewed?
        - Formally documented/recorded?
- Who drafts the evaluation report?
    - One person?
    - Wider range of sources/staff – are all relevant stakeholders included?
- Who approves the report?
- Are prisoners formally provided with the report?
- Is there a clear process by which prisoner can appeal against an evaluation report?
    - Yes – within process, or after report completed?
    - Only against measures taken on the basis of the report?

[1] For example, see pp. 4-7, https://static1.squarespace.com/static/5b3108bbe74940194b83f30f/t/5bc59e50e79c7018651e2c5f/1539677840014/Practitioner%27s+Guide+NGO+complaint+mechanisms.pdf

- How does the evaluation process work in practice?
    - Is it deemed reasonable fair by those that conduct it?
    - Is it deemed reasonable fair by prisoners/families?
    - Etc.

### 3.5 Example from the Albanian Immovable Property Registration System, 2010-2011

The assessment, conducted in 2010-11 was of IPRO (Immovable Property Registration Office - now the State Cadastre Agency). However, it necessarily covered aspects involving other institutions, such as ALUIZNI (Agency for Legalization, Urbanization and Integration of Informal Areas/Constructions), Restitution Agency, and the courts.

| Process | Activities (components of process) | Risks identified | Risks factors identified | Key recommended measures |
|---|---|---|---|---|
| **Provision of land title deed** | Maintaining records of land title (real estate registration) | | Lack of clear land policy<br><br>Incomplete records<br><br>Inaccurate records<br><br>Conflicting records held by different institutions<br><br>Use by IPRO of outdated manual processes | Formulate clear strategy and vision for land policy<br><br>Establish responsibility of only one institution for property registration/place all bodies under one authority<br><br>Establish clear duties and procedures for sharing information between various bodies<br><br>Ensure same/compatible technology across institutions processing land records<br><br>Adopt and adhere to IPRO Business Plan to establish self-financing, IT needs and investment, staff capacity building.<br><br>IPRO HR management: comprehensive |
| | Accepting requests for registration | Bribery to obtain documents from different institutions<br><br>Bribery in submission by citizens to IPRO of documents from other institutions | Number of documents required<br><br>No procedure established for (automatic) communication of property related records/decisions to IPRO | |
| | Processing requests for registration(IPRO) | Bribery in order to ensure: legitimate documents of ownership are accepted; registration decision that should not be made. | Ambiguity in law regarding which documentation establishes undisputed ownership<br><br>Insufficient training<br><br>Poor infrastructure and IT systems | |

| | | | | |
|---|---|---|---|---|
| | Issuing decisions on registration (IPRO) | Bribery/undue influencing of registration decisions at IPRO | No financial indemnification of victims of poor decisions | training programme, open and competitive recruitment, define status of IPRO employees, establish qualification requirements and certification, introduce and implement code of ethics.<br><br>Complete First Registration (and digitalisation of Land Registry), and speed up process by increasing transparency (e.g. put all records online for free).<br><br><u>Mitigation</u>:<br>Resolve problems in government Instructions to ensure clarity in case law approach of courts, IPRO actively engage with High Council of Justice on problems of case law |
| | Appeals against registration decisions (IPRO, courts) | Decisions not communicated to IPRO by other institutions<br><br>Citizens vulnerable to bribery pressure at IPRO when submit documents from other institutions | | |
| | Disputes over registration (IPRO, other institutions, courts) | Bribery at IPRO or courts to settle disputes<br><br>Courts failing to decide based on up-to-date IPRO documentation<br><br>Courts issuing declaratory statements of ownership without required supporting documentation, for property that was illegally privatised, or that infringes upon public property | Unclear procedures for property disputes, due to Government instructions being invalidated by court decisions<br><br>No procedure for automatic communication of documents from IPRO to courts (see above)<br><br>Very few staff who are lawyers to represent IPRO in court | |
| | IPRO human resources management | Recruitment based on non-professional/non-meritocratic criteria<br><br>Insufficiently competent staff<br><br>Inefficient and subjective decision-making | Inadequate standards on qualifications/conditions for hiring<br><br>Status of IPRO staff as non-civil servants<br><br>Hiring on short-term contracts<br><br>Very little training<br><br>Absence of performance standards<br><br>No code of ethics/conduct | |