Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Joint European Union – Council of Europe Project
"Strengthening the Capacities of Law Enforcement and Judiciary in the Fight against Corruption in Serbia" (PACS)
www.coe.int/pacs

Technical Paper

RISK ANALYSIS METHODOLOGY GUIDE

Prepared by Mr Robert Murrill, Council of Europe Expert, and
Mr Lado Laličić, Council of Europe Secretariat

May 2013

ECCU-PACS SERBIA-TP1-2013

Table of Contents

For any additional information please contact:

Economic Crime Cooperation Unit
Action against Crime Department
Directorate General I, Council of Europe
Tel: +381 11 71 555 12;
Email: lado.lalicic@coe.int; www.coe.int/pacs

This document has been produced with the financial assistance of the European Union and the Council of Europe. The views expressed herein can in no way be taken to reflect the official opinion of the European Union or the Council of Europe.

INTRODUCTION/EXECUTIVE SUMMARY

This paper provides a general outline of the proposed methodology to be used in identifying, analysing and assessing the key risks associated with the existence of corruption in the Serbian law enforcement, prosecutorial and judicial authorities. The methodology also provides a general outline on how the analysis could be carried out with regard to the risks arising during the process of investigation, prosecution and adjudication of corruption cases in Serbia.

The sectorial/functional diagnoses will identify specific individual and organisational vulnerabilities in relation to corruption. In this step, the assessment will look *across all of the sectorial and functional diagnoses* - this process will identify the key causes and consequences of the risks involved and will provide the opportunity to identify critical control measures. Recommendations can then be made as to the actions required to address the causes and mitigate the consequences of corruption. These recommendations shall then serve as a prioritisation platform for the Serbian authorities that have responsibility for implementing mainstream anti-corruption strategies and operations.

Furthermore, the adoption of this dual approach – to have parallel analysis of corruption related risks during the criminal proceedings and corruption risks within the institutions competent to run such proceedings - will lay the foundation for future work that will enable the development of the above referred recommendations and the introduction and application of the mitigation functions. The first stage of this process is intended to provide qualitative rather than quantitative assessment in that and it will identify the principle causes and consequences of corruption.

This paper has considered the work already carried out by the Serbian Ministry of the Interior in 2012 – a comprehensive report 'Strategic Intelligence Assessment on Corruption' conducted in cooperation with the UK Serious Organised Crime Agency (SOCA). With due consideration to the methodology upon which that assessment was made and the recommendations that will be made as a consequence of this report, this paper suggests that the report is used as a benchmark to assess progress to date within the Ministry of Interior. The report could also act as a template for reviewing the effectiveness of future initiatives undertaken not only for law enforcement but also for the judiciary and prosecution environments.

This paper provides an illustration of the application of 'bow-tie' methodology as it has been applied within other jurisdictions to the law enforcement environment. The methodology is approved by the Institute of Risk Management and is widely applied to both strategic and operational risk environments within the public and private sectors. Using this methodology risk assessors can provide a visual representation of the causes and consequences of risks and the relative controls and mitigations. Furthermore, the paper elaborates the methodology's practical implementation and results that it provides.

Finally, this paper will explain how the material gained at this stage can be later incorporated into a linear risk register, numerical weighting applied and risk analysed according to their impact and likelihood. This will enable the prioritised introduction of critical control functions.

TERMS AND DEFINITIONS

Risk

The International Organization for Standardization (ISO) established the first international risk management standard. The risk is defined in terms of the effect of uncertainty on objectives. 'An effect is a deviation from the expected positive and/or negative' (ISO/FDIF 31000:2009:1). This is the latest internationally available definition of risk and is used by police, law enforcement agencies and other organisations throughout the world.

Further to that ISO provides certain elaboration of the risk management and states that *'the principles that organisations must follow to achieve effective risk management have now been made explicit. There is much greater emphasis and guidance on how risk management should be implemented and integrated into organisations through the creation and continuous improvement of a framework. An informative Annex describes the attributes of enhanced risk management and recognises that while all organisations manage risk in some way and to some extent this may not always be optimal.'*[1]

Corruption

To assess the incidence of corruption in an institution, the following issue needs to be clarified or taken into account.

Whilst there is not currently an agreed definition of corruption numerous references are made by different international organisations and elsewhere to acts that are considered to constitute corruption. It is broadly understood that the term should be applied beyond acts of soliciting or accepting bribes. Transparency International states that corruption is the abuse of entrusted power for private gain. World Bank similarly defines corruption - the abuse of public office for private gain, the OECD defines corruption as an 'active or passive misuse of the powers of Public officials (appointed or elected) for private financial or other benefits' while some independent authors define corruption as a 'violation of non-partiality principle (Vito Tanci); and as a 'deviate behaviour of individual in relation to formal role (Nye and Khan).

Serbian legal framework on corruption

The first legal document that has a definition of corruption is the Serbian National anti-corruption Strategy adopted in 2005 by the National Assembly.

[1] http://sherq.org/31000.pdf

The Strategy defines corruption as a relationship based on misfeasance in the public or private sector with the aim to acquire gain for oneself or another.

In 2008, Serbian National Assembly adopted the Law on the Anti-corruption Agency that has almost identical definition of corruption as the one in the Strategy- it is a relation based on abuse of office or social status and influence, in the public or private sector, with the aim of acquiring personal benefits for oneself or another.

Criminal offences typically considered as criminal offences of corruption are located in the Chapter 33 of the Serbian Criminal Code - *Criminal offences against official duty*:

- Abuse of office
- Abuse of law by the judge, public prosecutor and deputy public prosecutor
- Embezzlement
- Trading in influence
- Accepting bribe
- Giving bribe.

With the latest amendments of the Criminal Code, adopted in December 2012, two new criminal offences are introduced into the Serbian legal system:

- Abuse of office by a responsible person
- Abuse in relation to public procurement.

Serbian system recognised so called *high level* corruption. This derives from the Law on Organisation and Jurisdiction of the Government Authorities in Suppression of Organised Crime which establishes the competence of the Prosecutor for organised crime when an accused, that is, a person receiving the bribe, is an official or a responsible person holding public office, on the grounds of the election, designation, or appointment by the National Assembly, the Government, the High Judicial Council, or the State Prosecutorial Council, as well as for the criminal offence of abuse of office when the value of material gain exceeds 200.000.000,00 RSD (approximately 1,800.000,00 Euros as of the date of this report).

Usually, a perpetrator of a criminal offence with the element of corruption is an official person or responsible person, or a person with the social power-politically exposed persons or members of family or friends of the politically exposed persons. However, these cases can also be considered as serious corruption although they don't necessarily have to be within the competences of the Prosecutor for Organised Crime.

The Council of Europe projects in different jurisdictions have applied risk assessment exercises in different sectors (i.e. AZPAC project in Azerbaijan, UPAC

project in Ukraine, PACA project in Albania[2], etc.) whereas the goal was to assess corruption and its prone areas within the institutions, the methodologies used also tackled the broader understanding what corruption practices are and to what the assessment shall focus on. In that sense, the following was offered by the Council of Europe Project against corruption in Albania – its Risk Assessment Methodology Guide stated that '*the risk assessment should not focus directly on corruption but, instead, to focus on specific practices within an institution that compromise that institution's capacity to perform its public service function in an impartial and accountable manner; Individuals with a public service role act in a way that serves their own interests rather than those of the public*.'

A broader interpretation is also adopted within a recent Strategic intelligence Assessment in respect of corruption within police structures in Serbia, which states that, *Although, corruption is usually related to accepting money, a high proportion of respondents (42.4%) think that corruption implies "any benefit gained by doing an illegal favour." A significant number of respondents recognise corruption as a "promise which will be remunerated by a favour" and "the use of official information to gain a personal benefit".*

The papers cited above support a general assumption that corruption and the perception of what type of behaviors constitute corruption, goes beyond acts of soliciting or accepting bribes. The approach to this risk process will therefore encompass this broader interpretation.

METHODOLOGY (and the order in which activity is to take place)

Data Collection

1. The risk analysis exercise shall start with the review of the already available documents. This includes, but is not limited to the existing legal framework, internal acts and regulations, previous analysis made by the institutions themselves and those made through the technical assistance projects and civil society organisations. Good example - a good starting point for such data collection when conducting risk analysis within police is the above-referred Strategic Intelligence Assessment conducted in 2012 by the Ministry of the Interior and SOCA. This data can be utilised to begin a benchmarking process and the data collection methodology shall be either adopted or adapted for the ongoing assessments. As far as it concerns judiciary and prosecution, the integrity plans, which these institution are, *ex lege*, obliged to submit to the Anti-corruption Agency could play an important role and, again, could serve as a starting point for the risk analysis exercise within these institutions.

2. Next step would involve examination of complaints submitted by citizens to Internal Affairs Sector(s), regional police directorates, courts and prosecutorial authorities, including here those submitted to the High

[2] http://www.coe.int/t/dghl/cooperation/economiccrime/corruption/default_en.asp

Judicial Council and the State Prosecutorial Council. The examination would need to quantify the number of complaints versus final decisions and also note what corruption practices were mostly presented in such complaints, with special attention to those that resulted in convictions, including here those convictions from the disciplinary proceedings.

3. Study of criminal charges filed against police officers, prosecutors and members of the judiciary for corruption related offences.

4. Conduct risk identification workshops with representatives drawn from the police, prosecuting service and judiciary. This step is necessary to identify additional risk areas that have not already been addressed and is an integral part of the ongoing process illustrated in figure 1.

5. Interviews (structured and non-structured) - a key source of information for any risk analysis is the conduct of targeted interviews with relevant persons: officials/agents/employees of the institution(s) concerned, interested parties/citizens, attorneys and other members of the experts community, and investigative journalists. It could be said that interviews are often the most important method for securing information on corrupt practices or other malfeasance. As suggested by the afore-mentioned PACA Corruption Risk Assessment Methodology Guide, *it is of very high importance to follow certain rules when pursuing this approach:*

In general, selection of interviewees should strive to avoid selection bias. However, it is unavoidable that selection will sometimes be 'biased', for example by targeting complainants to particular institutions. This may imply that the information gathered will indicate more extensive problems than in fact exist. In these circumstances, it is important for the interpretation of the information obtained to take into account such bias, to avoid unjustified generalisation, and to seek access to those who experience no difficulties with the institution.
Likewise, interview questionnaires should be designed in such a way that they will not elicit systematically biased responses, for example through 'leading questions' that implicitly suggest there is corruption whether this is the case or not ('putting words into the mouths of the interviewed').
Moreover, the standards of evidence need to be symmetrical between complainants and those accused, rather than assuming that there is 'no smoke without fire!'
Questionnaires should strike a balance between focusing specifically on issues identified by the risk assessment team, and providing interviewees with the opportunity to speak outside of certain constraints.
Having said that complaints and concerns that arise in the more open-ended parts of the interview need subsequently to be investigated with a similar degree of rigour as those identified by the risk assessment team, lest casual remarks are given disproportionate weight.

Once these five stages have been undertaken sufficient data will have been collected to start mapping out and identifying the key risks not previously identified, in relation to their causes and consequences.

Following completion of the initial data gathering a survey of key social groups will be designed and conducted. Consideration should also be given to the breadth of the survey to be undertaken and who should conduct it. The following outlines the steps that should be taken to design and conduct the survey.

- Map information gathered
- Write and test survey questions
- Identify and train surveyors

Once these steps have been made it will be possible to conduct a meaningful process for defining the Institutional Risk Questionnaire (italics indicate action in the Figure 1 below). The Institutional Risk Questionnaire content will be informed by the survey data gathered by the process below. Some already exists (SOCA 2010 and the Ministry of the Interior) but the feedback from the groups below will identify other areas that have not yet been addressed. Once this is gathered areas of vulnerability will be identified and inform further risk assessment activity.

- Survey of citizens
- Survey of police officers
- Survey of prosecution and defense lawyers
- Survey of Judges and Judicial staff
- Consultative process with relevant trade unions and professional bodies.

Process

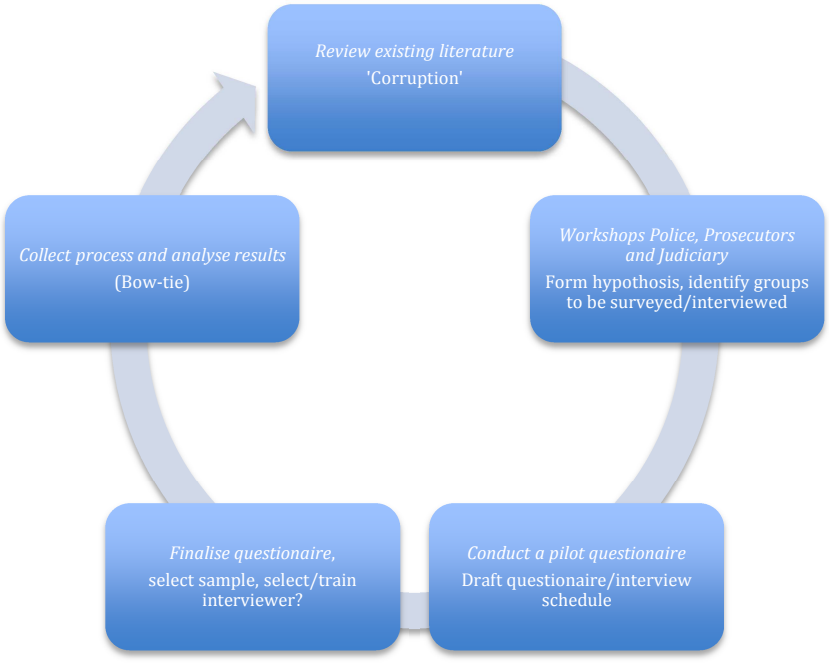


Fig 1
Taken from methodology outlined in McNeill and Chapman, 1985:29

CONDUCTING RISK ASSESSMENTS

Internal vs external assessment

Institutional risk assessments may be conducted by any person with the required expertise.

Ministries and institutions may complete the risk assessment questionnaire.

The assessment should identify risk factors whilst assessing the incidence of corruption and examining in more depth issues identified as important through the risk assessment questionnaire. Just as importantly, the risk assessment process will recognise areas of good practice which enables analysis to be undertaken to identify the conditions that exist and promote integrity.

Consideration should also be given to external partners organisations being tasked to carry out any assessment. This will provide a degree of independence and allow a baseline to be established against which all future progress will be measured using benchmarking within and between the bodies being reviewed.

Analysis and Modelling

Bow-Tie methodology will be initially used to identify the causes and consequences of risk associated with corrupt activity. The Bow-tie methodology in relation to risk management involves a visual diagram which portrays each risk using clear and concise imagery. The Bow-tie name itself comes in relation to the way the diagram visually looks and is set out - in the shape of a bowtie. The diagram shows all threats aligned to a risk and the purpose of each of the controls put in place to prevent it.

This methodology and modeling has been successfully applied within a broad range of high risk operating environments and law enforcement (Toyne, risk and operational security, MPS 2013). The Bow-tie provides an overview of the entire risk management process. This helps understanding the worst case scenario should a loss of control and undesirable event (risk) take place, the preventive controls in place to stop it and the recovery controls designed to minimise the impact should it occur. It means that the model provides the platform for future evaluation, monitoring and review of the impact of the control functions once they have been identified and applied. The absence of a process for evaluation, monitoring and review renders any risk management and mitigation measures meaningless.

Typically bow-ties are developed by asking a structured set of questions which build up the diagram step-by-step. Facilitated workshops involving people who are regularly confronted with the risks have proven to be the most effective way of identifying real controls and capturing past incidents and current practice. Openness is an essential ingredient during these sessions if any weaknesses in controls are going to be uncovered. To encourage free discussion, the workshop

needs to be run in an honest and engaging fashion and an independent facilitator can often help to create such an environment.
(Bow – tie model diagram as it would appear in relation to a corrupt relationship with an informant is presented on page 14 of this paper).

Case History Illustration

Through the case history illustration there will be two types of risk identified, those that actually exist and have occurred previously and those that are identified through the process but have not yet happened. Those that have already occurred should have mitigation controls already identified. Those identified but not yet occurred will have preventative control measure identified.

Case histories will be used to illustrate key findings and assist with drawing conclusions. The following provides an overview of the risks of corruption associated with police officers handling informants using causes and consequences analysis. Figure 2 illustrates how this information can be displayed on a single sheet or presentation while using the bow-tie methodology.

Following the findings of the risk assessment the following categories could be identified and elaborated.

Elements that cause corruption practices:

- Need – Insufficient income to support basic needs leading to employee taking money or other value to offset financial vulnerability;
- Greed – Large amounts of untraceable cash available to officers in course of duty – invitational edge of corruption;
- Lack of supervision leading to increased opportunity for operatives to indulge in corrupt activity without fear of detection;
- System demands to meet targets leading to operatives falsifying figures.

Consequences of corruption practices (police taken as an example):

- Officer takes money from informant;
- Officers submits false records to support payments;
- Possible compromise to innocent parties e.g. colleagues witnessing activity (in the UK in 1997 a number of police officers engaged in corrupt activity, stealing drugs from informants at the time of arrest. The amount seized by the corrupt officer at the time of arrest was known to all officers involved in the arrest but when charged later the same day, the quantity had been greatly reduced. This was known to the officers who had not been involved in the corrupt act and left them with two choices: to either go along with the corrupt act or report the act. This compromise of integrity led to the current 'whistleblower' policy).
- Agent provocateur activity - this relates to circumstances where an otherwise innocent person is asked to commit a criminal act when ordinarily they would not have done so. Such an activity would lead to the dismissal of the criminal case (e.g. an individual is asked by police to

obtain a firearm which they then obtain. This would be an act of 'agent provocateur'. If the individual had been asked **IF** they could obtain a firearm and then did so without further involvement with police it would NOT be 'agent provocateur' as the individual has acted of their own volition).

Preventative controls (police taken as an example):

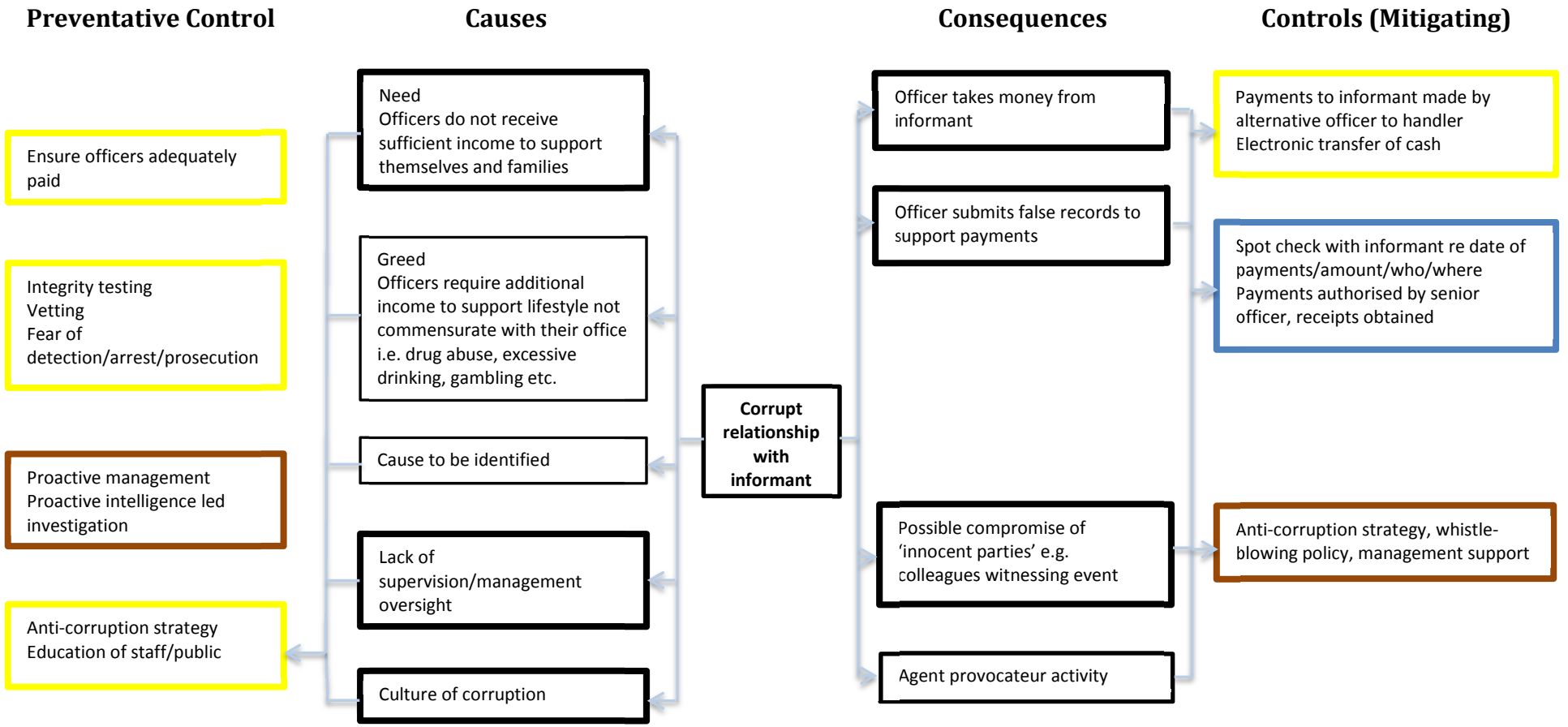
- No single handling of informants - the current guidelines for informant handling require two handlers to be present at any meeting with the informant. This is so any conversation or activity that occurs at the meeting can be witnessed and corroborated.
- Payments authorised by supervisory officer prior to being made - receipts obtained without proper records and authorisations it is possible for a corrupt officer to say they had made a payment to an informant and change the amount paid, keeping the balance for themselves. It has also been known for corrupt officers to ,make up, informants and then keep any reward money themselves. This ensures an audit trail exists of authority for payments which can be checked at any time by a supervisor talking with the informant.
- Payments made by another officer, not handler - another preventative measure that reduces the risk of the handler forming an inappropriate relationship with the informant and removes the handler from the proximity of any reward paid reducing the opportunity for corrupt activity by the handler.
- Informant 'owned' by organisation not individual – e.g. this required a cultural change in the UK where historically, officers ran their own informants who were never seen by supervising officers. By making the informant the 'property' of the organisation it was possible to allocate the informant to different handlers at any time, especially if there was a suspicion that the handler and officer were acting together in a corrupt manner. It also meant that if the officer left the organisation the informant was retained and was able to continue their work without interruption.

Mitigating controls

- Clear anti-corruption strategy – this means that each institution and/or its specific department shall prepare specific measures to prevent previously identified corruption practices;
- Education of staff – mandatory trainings shall be conducted within institutions and when necessary multidisciplinary trainings once corruption practices involve other institutions employees;
- Whistle blowing policy/procedure – either by country legislation or through institutions' internal acts the protection of all those signaling corruption malpractices shall be regulated;
- Electronic transfer of cash – this would ensure control over the money flaws and exact expenditures made;
- Need/greed – salary – as long as salaries are way below the needs corruption practices are likely to occur;

- Fear of detection/arrest/prosecution for corruption practices – in other words elimination of the 'impunity climate';
- Integrity testing - a keystone in any anti-corruption strategy is the fear of being detected and punished if discovered. Intelligence led integrity testing is key to supporting any organisation in fighting corruption. When intelligence is received that an individual may be corrupt and the intelligence is deemed to be credible an integrity test may be used to determine whether the intelligence is sound or malicious. Integrity Test may take the form of a simple test of honesty where money is handed in at the police station and the individual is expected to deal with it in a prescribed manner. It differs from any possible 'agent provocateur' activity in that whatever is required of the subject. It will always be up to them to do or not do the act. If the individual fails the test then a proactive operation against the individual may be conducted which will provide evidence to put before a court. The evidence of the integrity test itself will not be used as this is likely to compromise the methodology.
- Intelligence led proactive detection –– introduction and implementation of the concept of pro-active investigations which would include better usage of information gathered through intelligence work.
- Adoption of 'Zero Tolerance' principle in combating corruption;
- Vetting staff in sensitive positions - all staff who carry out sensitive functions within the organisation (e.g. witness protection, informant handling, intelligence analysts, case workers and who may be liable to be approached by criminals to either carry out or not carry out an act contrary to their remit) should be subjected to vetting procedures. Such a procedure will involve examination of their financial, personal and business interests, including their association with known criminals. Different levels of vetting are carried out dependent upon the risk attached to the subject. Usually, those involved in ant-terrorist activity will be vetted to a higher level than those involved in day to day crime investigations, as the risk of compromise and consequent outcome in the terrorist arena is higher.

Figure 2 Bowtie model as it would appear in relation to a corrupt relationship with an informant.



Restricted

By using this methodology it is possible to see at glance the causes and consequences of an identified risk and the recommended controls. The effectiveness of control measures can be reviewed and evaluated over a defined period and then adjustments can be made to reflect progress against the objectives set and any benchmarking adopted.

Checklists

As the bow-tie is developed the preventative and mitigating controls can be compiled into checklists suitable for application at both strategic and operational levels making it suitable for both senior managers and operational staff.

Risk Register

It is intended that the intelligence attained and assessed during this initial process will later be transposed into a strategic linear risk register. The purpose of the strategic risk register will be to identify 'risk owners'; those individuals and departments who will in due course be responsible for the allocation of actions and development of policy and procedures directed at controlling and mitigating the risks identified. These individuals will then be held accountable for the effective control of corrupt activity.

Conventionally a risk register will: -

- Identify the nature of a risk
- Identify controls that are in place
- Quantify the impact of the risk
- Quantify the likelihood of the risk occurring
- Provide an overall evaluation of the risk (impact x likelihood)
- Identify a person or department with responsibility for introducing controls
- Introduce additional controls
- Re quantify impact
- Re quantify likelihood of the risk occurring
- Evaluate residual risk (impact x likelihood)

Completion of the risk register (Annex A)

Once a risk has been identified it is scored from 1 – 5 for impact of occurrence, with low impact being 1 and high impact being 5. The risk is then assessed for likelihood of probability, again with low probability scoring 1 and high probability scoring 5. The scores are multiplied together to provide a numerical value for the risk. It is therefore possible to have a risk that is scored at 1 for low probability and 1 for low impact with an overall score of 1 (1x1=1) and a score of 5 for high impact and 5 for high probability with an overall score of 25 (5x5=25) or a score anywhere between the two. This method also allows for the risk to be

reassessed at any time e.g. when the risk has been subject to mitigation and the value changed reflecting its priority.

In the example provided in Annex 'A', the Likelihood score is 4 and the Impact score 5 leading to a risk score of 20 (4x5). After the mitigation control is applied the likelihood score has reduced to 1 with the Impact score remaining 5 giving a risk score of 5 (1x5). This reevaluation of risk allows resources to be redirected as necessary to other higher risk areas of activity. Additionally it provides corporate resilience and enables decision making to be articulated should an evaluation be challenged.

Once risk has been assessed it is allocated to a named individual responsible for dealing with the risk. Such a reevaluation should take place when any material change occurs related to the risk or at regular intervals (at least annually).

The matrix within Annex 'A' provides a quantitative representation that assists in measuring the level of risk and allows the assessor to articulate their decision making.

Serbia's Integrity Plan system

The Serbian Law on the Anti-corruption Agency defines that Integrity plans are adopted by the state bodies and organisations, territorial autonomy bodies and local state bodies, public services and public companies.

With the aim to implement these legal obligations, the Anti-corruption Agency (ACA) and the Government of Serbia signed the Memorandum of Understanding on 18 June 2010. By the Memorandum, the Government and public administration bodies are obliged to develop integrity plans in accordance with the guidelines published by the Agency, in the manner and within the timeframe prescribed. The Agency has produced and published Guidelines for the Integrity Plans Design and Implementation ("Official Gazette of RS", 80/10) in October 2010. The Guidelines define integrity plan structure, the way of developing plans through phases, performing particular tasks, timeframe for developing, method of monitoring the development and method of integrity plans implementation.

Integrity plan is a preventive anti-corruption measure- document that is being developed as the result of self-assessment of institution exposure to risks for corruption appearance and development, as well as exposure to ethically and professionally unacceptable acts.[3]

The Anti-corruption Agency's Handbook on integrity plans contains basic concepts of integrity plans such as its goal, importance, phases of preparation, assessment and evaluation of existing exposure, institutions obliged to develop them, working groups, measures to enhance integrity.

[3] Handbook for the development of Integrity plans, Anti-corruption Agency of Serbia

There is a clear correlation between the already existing Integrity plan system in Serbia and the Risk Registers as proposed above. In view of that, the integrity plans (those that concern police, prosecution and judiciary) will serve as a benchmark for the PACS project risk-analysis and will be taken into account through each phase of the implementation of the Risk-analysis activities.

Thus the project suggests that, apart from the aforementioned risk analysis and integrity plans, a benchmarking system aimed at measuring progress in suppressing corruption within the institutions is also established. This would enable further analysis and identification of problems that permanently occur. The Annex I to this paper on Benchmarking shows the role of the Risk Assessment in setting up the benchmarking mechanism, but also provides brief explanation of other steps needed in this process.

CONCLUSION

Whilst it would not be appropriate to identify the specific countries and agencies concerned, in advance of the initial research being undertaken, the methodological approach outlined above has been used to great effect in achieving strategic and operational control over high risk operating environments and activities. Apart from countering corruption these include:

- Undercover and covert policing
- Surveillance
- Informant/agent handling
- Witness protection
- De radicalisation programmes (these are multi-agency programmes directed at positively intervening when a person(s) are identified as being at risk of radicalisation.
- Community policing and managing multi agency The use of Risk assessments within the environment of multiple agency co-operation is highly effective in identifying areas where differing methodologies and operating procedures might lead to important activity being missed. Frequently, in multiagency initiatives, activity that is expected to be completed is found to have been omitted due to all agencies involved believing it to be another agencies' responsibility. Joint risk assessment between police and judiciary leads to identification of systemic errors and reduces poor outcomes when measuring success.

The benefits of an effective risk management process are universally recognised and include:

Internal benefits:

- Increased chance of achieving objectives by identifying areas of performance that require additional resource allocation or factors that inhibit delivery against objectives;

- Encouraging pro-active management by allocating specific risks to named persons and holding them accountable for all activity related to the identified risk(s);
- Identification and treatment of Risk leading to a reduction in risk to individuals and the organisation to whom they belong;
- Identification of threats and opportunities - by conducting e.g. a SWOT analysis (Strength/weakness/opportunity/threat) it is possible to identify opportunities to improve performance. Example: where an organisational risk is identified the allocation of the risk to an individual increases oversight and accountability and results in clearer lines of responsibility. It also provides the organisation with the opportunity to benchmark against similar sized organisations or similar sized internal departments.
- Compliance with legal and regulatory requirements and international standards;
- Improved local and strategic governance;
- Improved organisation learning, resilience and accountability.

External benefits:

- Improved stakeholder confidence and trust;
- Improved governance;
- Improved financial management;
- Improved resilience;
- Improved accountability;

The approach and methodology outlined above will identify the key causes and consequences of corruption risks and create the foundations for identifying and applying effective controls and mitigation activity.

In addition to the Council of Europe documents, this paper has been informed by the following publications:
National Police Decision Making Model (UK, NPIA, 2010)
Research Methods, (McNeill and Chapman, 1985)
Police Corruption *Deviance, accountability and reform in policing* (Punch, 2009)
Researching social life (Gilbert, 1992)
Risk (John Adams, 1995)
Politics of the police (Reiner, 2000)
Personal contact Mick Toyne (Risk Angels ltd)
Personal contact Aileen Quinton (Bow ties and Butterflys, strategic risk, IRM)
Perception of risk, (Slovic, 1998)
Trust, (Seldon, 2010)

ANNEXES:

- Annex I: Benchmarking
- Annex II: Sample Institutional Risk Questionnaire
- Annex III: Risk Register
- Annex IV: Risk Matrix

Benchmarking

Summary

> *'Standards of integrity can only be achieved in organisations that are committed to integrity and have embedded an integrity culture, have strong governance and oversight, understand the risks and opportunities and have appropriate measures to counter risks.'*[4]

The term integrity plan (or 'integrity programme') is used to describe the organisational system for integrity, the entirety of an agency's approach to managing integrity, including their anti-corruption policies and procedures. Their development in all agencies where there is any risk of corruption is a vital benchmark in measuring the progress of anti-corruption policies.

The following areas are suggested as key to the implementation of a successful integrity and anti-corruption approach. They have been developed mainly in the police sector. Police integrity is crucial in the fight against corruption - if the public know from experience that the police are themselves corrupt (for example if they accept bribes) they will be less inclined to trust them to deal with any report of corruption at all. As noted above, a survey in Serbia showed 74% of citizens believe that the police are too corrupt to investigate corruption, so corruption in the police needs special attention. However the principles inculcated can and should apply equally to any public body.

Clarity and consistency

The need for clarity and consistency cannot be overstated. All those charged with delivering or taking part in integrity management, or subject to such programmes, must be able to understand their roles and responsibilities.

Positive integrity management

Promotion of integrity, based on the principle of zero tolerance of corruption and pro-active detection of corrupt practices should be the adopted ethos of all involved in anti-corruption activity whilst simultaneously identifying and promulgating good practice utilised by employees. The issue of pro-active intelligence-led integrity testing has been examined within the UK law enforcement environment where it is seen as a key activity in preventing and detecting corrupt activity. It has also been adopted in Romania by the Anti-Corruption General Directorate (AGD). (We recommend in section 5 that it should be adopted in Serbia).

Common systems

All bodies involved in anti-corruption activity must adopt common standards

[4] Benchmarking police integrity programmes. ACPO, 22nd January 2013.

and terminology to ensure consistency of conduct and application which will enable all organisations to benchmark both internally and externally.

Governance and oversight

An independent structure for governance and oversight of the integrity plan is vital to ensure that the confidence of both employees and the public is instilled in the integrity process. Internal oversight, whilst important for the day to day governance of operational activity, does not instill the same level of public confidence of an independent review body. The following areas have been identified as best practice for good governance;

1. Focusing on the organisation's purpose and on outcomes for citizens and service users;
2. Performing effectively in clearly defined functions and roles;
3. Promoting values for the whole organisation and demonstrating the values of good governance through behaviour;
4. Good governance means taking informed, transparent decisions and managing risk;
5. Developing the capacity and capability of the governing body to be effective; and
6. Engaging stakeholders and making accountability real[5].

Model integrity code and tools

The implementation of a national integrity code should be supported by the use of model tools such as a typology of corruption and risks, analysis and monitoring procedures, self-assessment guidelines and a framework for public reporting. The adoption of such tools will ensure consistency of assessment and support both internal and external benchmarking.

Risk Assessment & Risk Registers

The risk assessment process should be robust, comprehensive and up-to-date in capturing emerging or changing risks. Regular reviews of identified and documented risks should be undertaken by identified 'risk holders' who must be held to account for progress (or the lack of progress) in dealing with corruption opportunities. Areas for consideration would include;

- Gifts and hospitality – introduction of a register and regular reviews

[5] *The Good Governance Standard for Public Service* (The Independent Commission on Good Governance
in Public Services 2004), p.7

- Associations – personal and corporate
- Business interests - notification and authority to conduct a business interest whilst employed
- Procurement processes – clear identification of lines of responsibility – procurement driven by a clear business case and need.
- Areas of vulnerability identified by the risk assessment process in conjunction with interested parties.
- Publication of identified corruption vulnerabilities and mitigation allowing benchmarking

Corporate attitude towards corrupt activity

There should be a zero tolerance policy with strong action against those found to be engaged in corrupt activity. This should be balanced with the potential for rewarding those who report such activity ('whistleblowers') and thus reinforce the zero tolerance approach[6]. Even the smallest of violations of integrity can undermine an anti-corruption policy.

Transparency of policy

For any integrity and anti-corruption policy to be successful it needs to instill in those who are subject to it, or beneficiaries of it, a belief that it is necessary, fit for purpose and delivers against published objectives. Transparency of such a process, by publication in the public arena allows for such confidence and supports measurement, peer benchmarking and tracking of improvements.

Context

Serbia's application to accede to the European Union shone the light on internal and external areas perceived to be corrupt or lacking in integrity. Consequently, a Strategic Intelligence Assessment (SIA) was carried out in 2010 conjointly by the Serbian Ministry of the Interior and the UK's Serious and Organised Crime Agency (SOCA)[7]. The findings indicated that respondents, including police, citizens and trade unions, regarded Health care as being the most corrupt area of society with the judiciary second and police third. The European Union therefore made improving Serbia's ability to successfully impact upon corruption a precondition to accession.

Methodology Utilised within the SIA

- Data collection was made using the following methods:
  - Survey of citizens
  - Survey of police officers

[6] Provisions on rewards are included in the current draft Serbian whistleblowing law
[7] The full report and analysis is attached to this report at Appendix A.

- Study of criminal charges filed against police officers for corruption-related offences
- Examining complaints submitted by citizens to Internal Affairs Sector and regional police directorates
- Review of public domain material on police corruption.
- Trade union contribution

An organisational approach to benchmarking corruption

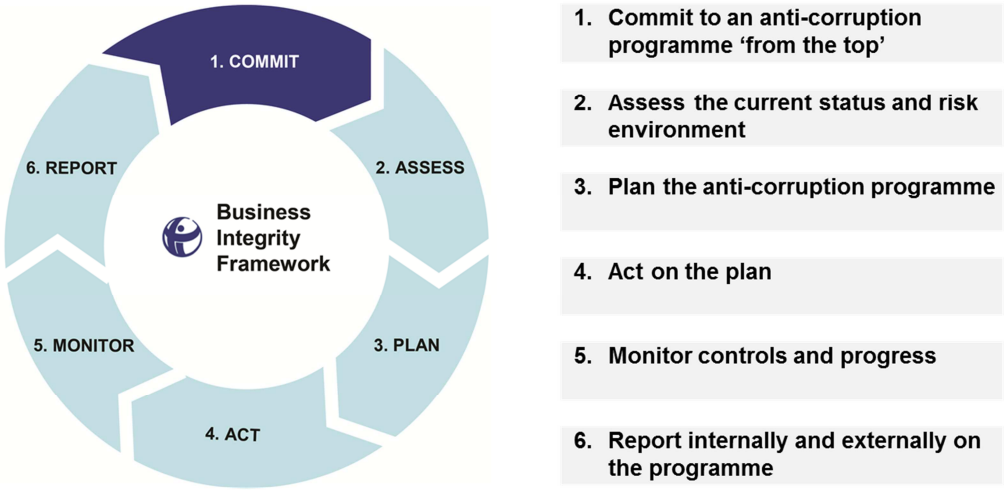


Figure 1: The integrity cycle used by Transparency International

Recommended steps to support an integrity plan that supports benchmarking

Key to any successful integrity plan is the need for 'buy-in' at the most senior levels of public institutions and government. Such a plan needs to be both publicly declared and supported, ensuring the public are aware that government and the institutions that represent them are fully and consistently committed to delivering success in the battle against corruption. The steps required for successful implementation that aid subsequent benchmarking are listed below.

Commitment

- Publicly communicated integrity values and zero tolerance of corruption
- Commitment to implement an integrity programme
- Definition of scope

Assessment

- Risk assessment

Plan

- Organisation and responsibilities
- Design of detailed policies and procedure

Implement

- Governance
- Leadership and oversight
- Policies and procedures implemented
- Management of key forms of integrity risk
- Associates
- Internal communication
- Training on the programme
- Human resources alignment to the programme
- Advice and whistleblowing channels
- External communication
- Public reporting
- Stakeholder engagement
- Collaborative working
- Sanctions

Monitoring, review and iprovement

- Internal controls
- Self-assessment and monitoring
- Audit – internal and external

Reporting

- Public reporting on aspects material to stakeholders (internal & external)

Transparency and public visibility of activity

Public reporting is vital, as it informs the public what anti-corruption measures an organisation is taking, whilst evidencing that organisation's commitment to anti-corruption. The European Code of Police Ethics states:[8] 'The police should be as transparent as possible towards the public. A readiness by the police to disclose information on its activities is crucial for

[8] *European Code of Police Ethics* (Council of Europe, 2001), p. 43.

securing public confidence.' This is affirmed by another report which says 'Police activity must be open to observation and regularly reported to outsiders. Police need to be accountable for their use of state resources — both fiscal resources and their use of their legal powers.' [9]

Benchmarking methodology – the requirement for consistency

During the scoping exercise conducted between 18 – 19 April 2013 it was established that whilst statistical data was available from the public bodies visited, it lacked consistency in both the type of data and reasons for its retention.

Nevertheless, the data obtained by the SIA in 2010 by the Ministry of the Interior is a good starting point, enabling the methodology utilised to gather the data to be repeated within a relatively short time frame (subject to appropriate resource allocation) and a benchmark to be obtained specific to that ministry. Such an exercise will provide not just information on the overall trends within the ministry but allow analysis to be undertaken from within the specific participant groups e.g. police, citizens and trade unions.

Publication of the results (regardless of what they show) will promote transparency and illustrate the commitment of the Serbian government to a more open approach and level of commitment to eradicating corruption and increasing integrity within the wider community.

Similar assessments should then be conducted within other public institutions to provide an initial baseline score. The importance of consistent data collection methods and terminology will ensure comparisons can then be made not just with longitudinal studies within the same institutions but between institutions, allowing the identification of best practice whilst also identifying poor performance.

Whilst it has been suggested that this project begins with a further assessment of progress made within the Ministry of the Interior since 2010, it is accepted that some public institutions may have made greater progress in the intervening years and would wish to promote their success. It is suggested therefore that the table illustrated in figure 2 be used as a baseline for such activity with those institutions being encouraged to adopt this checklist as a starting point and to enable meaningful data to be captured.

A simple scoring mechanism should be introduced to enable early comparisons e.g.

Commitment: - Does the organisation have a Publicly communicated integrity values and zero tolerance of corruption?

Good evidence	= 1
Partial evidence	= 0.5
No evidence	= 0

[9] *Recognizing Values in Policing* (Mark H. Moore, Washington DC: Police Executive Research Forum, 2003).

Stage	Good practice elements of an integrity plan	Evidence?
Commitment	Publicly communicated integrity values and zero tolerance of corruption	**[1, 0.5, or 0]**
	Commitment to implement an integrity programme	
	Definition of scope of integrity	
Assess	Risk assessment	
Plan	Organisation and responsibilities	
	Design of detailed policies and procedures	
Implement	Governance	
	Leadership commitment	
	Policies and procedures implemented	
	Management of key forms of integrity risk	
	Associates	
	Internal communication of the integrity programme	
	Training	
	Human resources alignment to the programme	
	HR: Vetting (as part of recruitment)	
	HR: early intervention	
	Advice and whistleblowing channels	
	External communication	
	Public reporting	
	Stakeholder engagement	
	Collaborative working	
	Sanctions	

Figure 2: Benchmarking Integrity Plans[10]

[10] Adapted from 'Benchmarking police integrity programmes' (Association of Chief Police Officers [UK], 22 January 2013).

Sample Institutional Risk Questionnaire[11]

Introduction

The following questionnaire is an example of the type of questions that might be utilised as a means for conducting a basic corruption risk assessment or good governance risk assessment. Different elements of the questionnaire will apply to different parts of the organisations being assessed. The questionnaire should be completed either on a self-assessment basis or by an external partner experienced in conducting such assessments.

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 descriptions/terms of reference and are staff aware of this?

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?
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 organisation receive income from the public or designated clients (taxation, customs levies, payments for services, fines etc.) What is the process for recording, banking and auditing these payments? In what form are such payments received?

[11] taken from 'Corruption Risk Assessment Methodology Guide' prepared within the framework of the joint CoE-EU Project against Corruption in Albania

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 police officers)?
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. State Secretaries
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 Civil Servants?
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 the 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?

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, fines 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?

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?

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 and contact persons
b. Ministry/institutional policies and policy documents
c. Laws and sub-legal acts
d. Draft laws and regulations
e. Procedures of relevance to citizens and legal entities
f. Statistical records?

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 Free Access to Information?
41. How many requests were filed last year?
42. How many requests were refused or are currently in dispute?

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 does 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?

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) and 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)?

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 from 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)?

Complaints mechanisms

61. Are there clear procedures by which citizens may file complaints against actions of the 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?

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)?

Vulnerable areas

69. Can you identify which areas of your organisation or its activities are most vulnerable to misconduct?
70. Has a risk analysis/integrity planning been conducted on your organisation to identify areas vulnerable to misconduct?
71. Does your organisation's Anti-corruption Strategy/Action Plan contain specific measures to tackle these vulnerabilities?

Anti-corruption policies

72. Who in your organisation has formal and specific responsibility for development, implementation, monitoring and coordination of anti-corruption policy?
73. Is this responsibility stated in that staff member's job description?
74. Is there a working group within the organisation tasked with formulation, coordination, monitoring and reporting on anti-corruption policy?
75. How often does the working group meet?

SERBIA CORRUPTION RISK REGISTER

Aim

Overall aim of activity (terms of reference for team)

Objectives

ESTABLISHMENT OF RISK REGISTER

Risk Heading	Nature of risk	Cause of risk	Existing controls	Matrix Impact x Likelihood = Risk			Planned controls	Matrix Impact x Likelihood = Risk Residual risk			Risk Owner and link to performance
				I	L	R		I	L	R	
Reputation	Money taken from informant	Lack of Supervision and Management oversight	Minimal	**5**	**4**	**20**	Intrusive management oversight and spot checks	**5**	**1**	**5**	**Leadership & direction**

Risk Matrix

Likelihood	Scale	Descriptor
Very Low	1	Unlikely to occur No record of previous occurrence; Assessed at 0 – 20% chance of occurring; Not likely to occur within next 24 months
Low	2	Potential to occur Has occurred but not in past 12 months; Assessed at 21 – 40% chance of occurring; Likely to occur within next 12 – 24 months
Medium	3	Possibly will occur Has occurred within last 12 months; Assessed at 41 – 60% chance of occurring; Likely to occur within next 12 months
High	4	Probably will occur Has occurred within last 6 months; Assessed at 61 – 80% chance of occurring; Likely to occur within next 6 months
Very High	5	Almost certain to occur Has occurred within last month; Assessed at 81 – 100% chance of occurring; Likely to occur within next month

LIKELIHOOD SCORES						
	Very High (5)	5 (Low)	10 (Medium)	15 (Medium)	20 (High)	25 (High)
	High (4)	4 (Low)	8 (Medium)	12 (Medium)	16 (Medium)	20 (High)
	Medium (3)	3 (Low)	6 (Low)	9 (Medium)	12 (Medium)	15 (Medium)
	Low (2)	2 (Low)	4 (Low)	6 (Low)	8 (Medium)	10 (Medium)
	Very Low (1)	1 (Low)	2 (Low)	3 (Low)	4 (Low)	5 (Low)
OVERALL RISK RATING SCORE		Very Low (1)	Low (2)	Medium (3)	High (4)	Very High (5)
		IMPACT SCORES				

Score	Rating	Action
20-25	High	Do not proceed unless an absolute operational necessity, in which case ensure high levels of monitoring control and support are applied.
8-16	Medium	Proceed with caution. Where operationally viable seek controls to reduce risk further. Ensure adequate and effective controls are applied.
1-6	Low	Proceed. Monitor for any significant changes. Look for options to turn threats into opportunities!

Checklist Content

The content of the issues checklist will arise from the material gained during the review, workshop and survey process however, the table below is provided as an example of how the checklist might appear.

Law enforcement	**Prosecuting agencies**	**Judiciary**
(Specifically, informant handlers)		
Finance		
Officers are adequately paid Vetted for role Trained and accredited		
Culture Proactive management Integrity testing Authorised meetings Authorised payments Knowledge policy/procedure		