UNDP

Empowered lives.
Resilient nations.

MANUAL ON INTEGRITY PLANNING AND INTEGRITY MANAGEMENT

2015

References to Kosovo in this report shall be understood to be in the context of Security Council Resolution 1244 (1999).
The designations employed and the presentation of material throughout this report do not imply the expression of any opinion whatsoever on the part of UNDP concerning the legal status of any country, territory or area or its authorities, or concerning its frontiers or boundaries.

The Manual on Integrity Planning and Integrity Management (2015) has been developed by the UNDP Public Administration Reform (PAR) in Kosovo project, with the support of the Government of Norway. The publication of the manual is supported by the Swiss Agency for Development and Co-operation (SDC) in Kosovo, thorugh the UNDP Support to Anti-Corruption Efforts in Kosovo (SAEK) project.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Cooperation Office Kosovo

ACKNOWLEDGMENTS

Author: Milena Minkova,
Expert on Integrity Management Systems,
Support to Anti-Corruption Efforts in Kosovo (SAEK), UNDP Kosovo

FOREWORD

When referring to a person as a "person of integrity", this means being honest, brave, moral, fair, professional and positive, as virtues formulating a person of integrity.

In the institutional aspect, integrity consists of several characteristics, such as: accountability, transparency, resistance against corruption, ethics and honesty, efficiency and public administration professionalism, whereas all of these entail the state efforts to improve the quality of public administration and to avoid corruption.

Kosovo public institutions face many risks of corruption that may have adverse impact in their functioning and public confidence.

A program of integrity needs active and strong, central and local support from political and professional leaders of public administration. They should set an example for all other individuals working in central and local institutions. I believe that Kosovo society welcomes a program of integrity and wishes to be a partner, whereas, the political part and employees in public administration should consider the program of integrity as support for professional accomplishment of their public tasks.

As a result, Anti-Corruption Agency, with its entire aptitude, works closely with the UNDP Office in Kosovo to develop the Integrity Management System (IMS) with the idea to help public institutions in addressing identified integrity systemic risks, as well as strengthen institutional resistance against corruption.

Kosovo has already marked the first step towards building integrity policies by forming the foundation to create an administrative culture of integrity in the Kosovo Anti-Corruption Strategy 2013-2017, approved by the Assembly of Kosovo. In this regard, drafting integrity policies in every institution in order to raise awareness on the risk from corruption, is an irreplaceable action.

As already known, the Municipality of Prishtina/Priština, Municipality of Gjakova/Đakovica and Municipality of Gjilan/Gnjilane have drafted and committed to implement the Integrity Plan.
In this regard, the engagements for distributing the IMS in municipalities are continuing and we hope that this example will be successful.

The staff of the Agency is strongly committed to assist all public institutions interested in drafting integrity plans, whereas we know for sure that the publication of this manual represents a valuable roadmap that particularly serves in the view of increasing integrity standards of public administration.

We believe that this Integrity Manual will be another contribution to the war against corruption in order to bring back the citizens' confidence to the work of Kosovo institutions.

Hasan Preteni,
Director of the Kosovo Anti-Corruption Agency

Contents

1 ABOUT THIS MANUAL

Throughout the public sector worldwide, there is a growing mandate to improve integrity planning and enhance integrity risk management. Why manage integrity risks and conduct integrity planning?

Public sector organizations in all countries at all levels face corruption risks that may have massive adverse effects on the achievement of their objectives. The more sophisticated these risks become, the greater the challenges they put to organizatons achieving their objectives and sustaining public credit. Integrity risk management is, therefore, the process whereby organisations methodically address the integrity risks attached to their activities with the goal of strenghtening organisational resistance to corruption and thus, reducing corruption levels. Integrity risk is being defined as effect of uncertainty on (organizational) objectives caused by corruption and integrity violations (Adapted from ISO Guide 73:2009, definition 1.1); while integrity planning is understood as the overall process of integrity risk assessment and developing risk based integrity plans in accordiance with integrity objectives/ commitments and integrity targets.

1.1 Why Integrity Planning

Traditionally, integrity risks have been identified and assessed centrally through a top down approach that focuses on the achievement of objectives, protection of assets, and/or checklists of commonly found integrity risks. Such standardized one-size-fits-all anticorruption approach has proven largely ineffective. Prevailing experience shows that integrity risks, which arise from the incentives and opportunities of individuals and their ability to evade internal controls, because of their complexity and specificity, are not easily identified through the top down approach even if there is both a will and a sufficient capacity in place. The above deficiencies escalate in scope and in effects once the planning of anticorruption (hereinafter, AC) strategies, action plans and measures is done in a framework, where capacities and political/ managerial will to counteract corruption remain of serious concern.

The above leads to the development of anti-coruption strategies/ plans/ measures that are detached from the actual vulnerabilities, projected on assumptions rather than on actual needs. Deficiencies motivated a search for effective instruments

to counteract corruption and manage integrity at an organizational level. This promoted an understanding that effective AC strategies have to be tailored to the specific environment in which corruption occurs, where planning of AC measures is built on a detailed country-specific and organization specific assessment of the system vulnerabilities to corruption. This must include a structured process of integrity risk assessment at the organizational level to (1) identify risks-determine where corruption is likely to occur and will impose the greatest costs, (2) assess the level of risk by assessing the probability of occurrence and the damage levels related, (3) set priorities in the intervention required and (4) develop organizational specific integrity plans that contain targeted anti-corruption measures.

Current evidence demonstrates that integrity risk assessment has become the basis for improved integrity planning in increasing number of countries (EU Member States, as well as in some candidate and accession countries). Although methodologies differ from country to country, the basic principles remain the same, in line with the relevant international risk management standards and lead practices.

1.2 Integrity Planning in Kosovo

Integrity planning has been put as a strong emphasis in both the Kosovo Public Administration Reform and the Anticorruption Strategies. These strategic documents reinforce the critical importance of a sustained process of integrity assessment in prevention of integrity violations and point to the need to introduce an appropriate integrity framework: supporting regulation and methodological tools. Adequate capacity building is considered important to sustain successful implementation. Institutionalizing corruption risk assessment and integrity planning within the Kosovo public administration sector would require a functioning supportive legal and operational framework. Its sustainability demands appropriate ownership of the process assumed by key stakeholders in anticorruption and integrity protection.

1.3 The Manual

This Manual is to support the introduction of integrity planning in Kosovo. It provides a brief overview of the key principles and concepts of integrity risk management and integrity planning, and highlights the process of planning, developing, implementing, monitoring and reviewing integrity plans. Its primary purpose is to translate the message of the importance of developing appropriate knowledge, experience and culture of integrity risk management, as well as the enabling mind set. The Manual is primarily an awareness raising tool, and has to be used along with further, more detailed methodolocical instruments and guidelines if an integrity plan is to be developed.

2 INTEGRITY, INTEGRITY RISKS AND INTEGRITY MANAGEMENT

2.1 Integrity as a standard

has already become a standard against which individuals, institutions and even countries are being assessed. With the growing importance attached to combatting corruption and safeguarding integrity, stakeholders worldwide are increasingly requiring assurance that organizations operate an integrity management system that is being based on a vigorous integrity risk assessment and thus, pursue its aims in an ethically sound environment. This is especially so in the public sector where the implementation of adequate anticorruption measures is becoming a condition for effectiveness, efficiency, transparency and accountability of institutions to determine levels of public trust and thus, gauge public political choices. A functioning integrity management is intensively recognized in the private and non-institutionsal sectors as well, perceived as a key to reduce oustanding economic and human costs of integrity violations, to enhance future business and boost organizational reputation and credibility. Assuring integrity then becomes instrumental to the organization's ability to fulfill in practice its commitments to stakeholders, with integrity planning being its fundamental pillar.

2.2 Integrity v/s Anti-corruption

Integrity is a broader concept than anticorruption. It has everything to do with social and professional interaction and co-operation between people, and with acting in compliance with the accepted values and standards.

To define integrity, the dictionary uses the words 'honesty' and 'incorruptibility';. something or someone who 'has not been touched' in the sense of being unaffected, untarnished, unblemished or intact. In Latin, 'not touch' (in tangere). Some management standards define integrity as "the total set of values, attitudes and attributes of an organizational unit which enables rigid adherence to a Code of Conduct and to ethical behaviour."

Any organization may easily be discredited once its integrity is violated. Integrity violations include, but are not limited to:

- **Conflict of (private and public) interest;**
- **Fraud and Theft;**
- **Corruption;**
- **Misuse and Manipulation of Information;**
- **Incompatible Functions, Activities;**
- **Improper use of Authority;**
- **Waste and Abuse of Resources;**
- **Discrimination and Sexual Harassment;**
- **Private time misconduct.**

2.3 Where do integrity risks occur

Integrity risks can occur in most areas of functioning of a public sector organisation. They relate to probability of occurrence of events related with corruption and integrity that will prevent the organization from achieving its objectives. Commonly perceived high risk areas include, but are not limited to:

- **Management of funds and financial resources (allocation, control and audit of budgets, management of assets, payment of expenses, granting bonuses, etc.)**
- **Handling of information (holding insider information, provision of confidential information; production, supervision, storing, duplication of confidential information, incl. electronic files and database, internal and external mutation of confidential information, incl. electronic files, etc.)**
- **Management of goods and services (making decisions about purchasing, setting quality requirements in terms of delivery, assigning suppliers, administration and allocation of goods within the organization, using company goods in non-office hours or outside the organization)**
- **Human Resource Management (HRM) and Human Resource Development (HRD) (recruitment and selection of personnel; attestation of staff; making decisions on carrier development; training assignments; study tours, etc)**
- **Granting rights (licenses, approvals, permission regimes, authorization, certificates, etc)**
- **Collection of payments (taxes, administrative charges, amounts due, etc)**
- **Contracting (orders, tenders, contracts, etc)**
- **Payments (premiums, allowances, sponsorships, benefits, etc)**
- **Enforcement of legislation (Control, supervision, compliance checks, imposition of sanctions, penalties, etc)**
- **Operations management;**
- **Cash Management; General expenditure**
- **Other areas with public interface where discretion is being exercised and related opportunities exist.**

2.4 Can we manage integrity risks

Available instruments to manage integrity risks can be feautured by a growing diversity and specialization. These include, but are not limited to legal regulations and code of ethics; integrity management systems; control-based tools; anti-corruption audits; integrity risk assessment and integrity planning. Within this diversity of approaches; there is no instrument that is a panacea solution to effectively curbing corruption. Instead, there are instruments that are better suited to particular environments based on existing capacities, record, specific environments, etc. The related costs of implementation appear different as well. Therefore, a copy paste approach of a mechanic transfer of working practices across different contexts should be preceded by an in-depth analysis and needs assessment to determine the tools that will be best fitted to the unique organisational environment. Whatever instruments are used, the ultimate goal is to make corruption a "high risk" and a "low return" undertaking. The integrity management systems are designed to prevent corruption from occurring in the first place, rather than relying on penalties after the event. Maintaning the appropriate balance between prevention v/s repression becomes critical for effective anticorruption and integrity prevention.

3 THE INTEGRITY PLAN

The Integrity Plan is a strategic, as well as operational document, that substantiates the results of a systematic integrity risk assessment process undertaken within an organization. It is based on identification of risks, risk analysis and evaluation; and specifies risk based measures for achieving its integrity objectives to enhance integrity performance of the public administration sector and reinforce the rule of law and professional values and standards. The Integrity Plan is to be seen not as a static, but as a living document, which implementation would need to be monitored in a planned format, periodically reviewed and updated in accordance with the relevant normative, institutional, procedural and personnel developments within the changing organizational external and internal environment.

Thus, the integrity plan presents

- ***a preventive*** **anticorruption strategic tool to strengthen the integrity of the institution, which includes individual integrity, professionalism, ethics, institutional integrity, as well as adherence to moral values and professional standards.**
- **an instrument for increasing *awareness* about organizational vulnerabilities and exposure to integrity violations, as well as for generating support to measures that aim at enhancing its resilience to corruption and building a climate of trust and co-ownership in anticorruption across the organization, involving all levels and all functions**
- **a natural, inherent *part of the overall management* of the organization**
- ***a living*** **document, part of the organizational learning.**

3.1 Purpose and Objectives

Integrity planning is considered to be **instrumental** for the public sector organizations to:

- **Increase the likelihood of *achieving organizational objectives*, encourage *proactive* rather than reactive integrity risk management; *minimize loss* from corruption and integrity violations, *reduce/eliminate opportunities for corruption and improve organizational resistance* to corruption;**
- **Improve identification of opportunities and threats and treat risk throughout the organization; focus on prioritities, *improve controls; establish a reliable* basis for decision making and planning by *effectively allocating and using resources* for risk treatment in the integrity plan;**
- **Ensure *compliance* with relevant legal and procedural requirements and international norms and standards;**
- ***Create/strenghten capacities* of staff for effective anticorruption, build awareness at all levels and create *co-ownership* in the process of developing, implementing and monitoring integrity plans;**
- **Improve external and internal stakeholders' *confidence and trust* and respond to their *requirements and expectations* as regards to the integrity performance of the public sector.**

The Integrity Plan is built on an organizational analysis and does not pursue to identify the current state of integrity within a specific unit, particular corrupted areas or corrupted persons within the system. Accordingly, it is not to be seen or/and felt as a format of "witch hunting", but as a part of the organizational development of the organization where it focuses on effective integrity risk taking to improve its integrity performance and public image. Thus, it does not directly address the integrity of individuals, but establishes mechanisms to prevent and eliminate conditions for the occurrence of corruption, unethical and unprofessional practices in all areas of the functioning institutions involved.

The specific objective is to raise awareness of the vulnerabilities related to corruption, and promote the "zero tolerance to corruption" approach. Developing an integrity plan involves an assessement of the effectiveness of the institutional integrity management system, including quality of regulations, personnel practices and processes in all areas of operation (governance, financial management, human resources, procurement, information security, assets management, etc), it could be a decisive step towards improved management and performance in these areas. Importantly, it promotes a participatory approach of all staff, based on the assumption that risk is best known to these involved directly in implementing the activities.

3.2 Contents of Integrity Plan

The Integrity plan shall consist, in particular, of:

- **Data on the organisation, brief profile of the internal and external environment as regards integrity, applicable risk criteria (usually "zero tolerance" to corruption approach) that may be incorporated in an Integrity Statement;**
- **Results from identification of integrity risks and their analysis; measures for timely detection, prevention and elimination of corruption risks and their implementation;**
- **Integrity Action Plan/Risk register, including proposed measures, responsibilities and deadlines.**

4 HOW TO APPROACH INTEGRITY PLANNING?

4.1 Continuous and systematic process

IIntegrity risk management is a continuous process which runs throughout the organisation's strategy and the implementation of that strategy.

Being a critical part of the integrity management, integrity planning addresses methodically all integrity risks surrounding the organisation's activities past, present and in particular, future. Thus, it should not be perceived as an incidental exercise in assessing risks and preparing an integrity plan, but rather a long term commitment undertaken to enable sensible and effective integrity risk taking.

4.2 Resourcing integrity planning; Responsibilities

Successful implementation of integrity planning requires adequate resourcing. This includes human, as well as financial resources. Organisations should therefore allocate sufficient resources to both the development of the integrity plan, as well as to its further implementation.

The cost of treating risks is often underestimated in the integrity planning process. Over ambitious plans that fail to set priorities and to understand the impact of the potential cost of treating risks may lead to increased pressure on the personnel involved, on the available organisational budgets, whereas any consequent deficiencies in implementation reflect on the reputation or credibility of the organisation.

It is critical to identify personnel to implement the integrity plan and to manage it on an ongoing basis. Organisations that demonstrate good risk management practices are those that have identified an individual or team to oversee the implementation and facilitation of the integrity plan. Responsibilities to integrity planning and to overall integrity management, however, extend beyond the pool of those that have been directly mandated with its development, but include all employees in the organisation, in accordance with their level of competence and responsibilities. Thus, integrity needs to be managed at each level, by anyone working for the organisation or on its behalf.

Top Management	Top management shall provide evidence of its commitment to the development and implementation of the integrity planning process and continually improving its effectiveness by: » Providing the resources needed to establish, implement, maintain and improve the integrity planning process; » Communicating to the organization the importance of meeting integrity standards as well as legal and other requirements; » Having ensured that risk based integirty plan(s) are established; » Having ensured that results as regards implementation of the integrity plans and the integrity performance are measured and reported at planned intervals
Senior Management	» Review organization wide and department specific risk profiles » Review and assess the current and planned approach to managing significant and critical risk areas. » Review and monitor completion of risk based integrity plans. » Ensure the risk management framework is implemented in individual operation units.
Auditors / Cotrollers / Inspectors	» Oversee the risk management process » Contribute to identification of integrity risks in the organization key processes.
Integrity Planning Working Group	» Plan, organize, conduct, document, communicate and report integrity risk assessment and integrity planning
Managers and Supervisors	» Facilitate, challenge and drive the integrity planning process within the organisation » Monitor risks and risk management in their areas of responsibility » Ensure staff are adopting the integrity planning framework as developed and intended » Report to the top and senior management staff at regular intervals
Employees	» Recognise, communicate and respond to identified and emerging risks » Contribute to the process of identification of risks for their operational unit » Implement risk plans within their area of responsibility

The head, respectively, the person in charge of the overall management, of the obliged persons (hereinafter, head), who holds the *ultimate responsibility* for integrity management within the organization is responsible for the integrity planning preparation, development, approval and implementation.

Setting Up a Working Group on Integrity Risk Assessment and Integrity Planning

A good risk assessment requires input from various sources. It demands adequate resourcing and organization. Therefore, before conducting a risk assessment and initiating integrity planning, the Head of the obliged entity issues a decision that the organization shall conduct integrity planning, nominates a team leader and members of WG on integrity planning.

The appointed members (usually, 5-9) should be officials from throughout the organization with different knowledge, skills, and perspectives, representatives of different positions / areas of activity, such as legal and compliance personnel, internal audit personnel/ inspectors/ investigators, accounting/finance personnel, nonfinancial business unit and operations personnel, who have knowledge of day-to-day operations, customer and vendor interactions, and general awareness of issues within the sector. Management, including senior management, and significant process owners (e.g., procurement, inspections, legal and compliance, operations) should participate in the assessment, as they are ultimately accountable for the effectiveness of the organization's risk management efforts.

If expertise is not available internally, external consultants with expertise in applicable standards, key risk indicators, integrity risk management and integrity planning methodology, control activities, and detection procedures may be used on a limited scale. The organisation shall bear in mind, however, that risks are best known and managed at the place of business, an intimate understanding of the work processes is critical to effective risk identification and risk management.

The WG on integrity planning shall plan, organize, conduct, document, communicate and report integrity risk assessment and integrity planning.

The Leader of the Working Group is to manage the integrity planning process, define and communicate related responsibilities and authorities; organise activities and schedule; promote awareness of the integrity planning at all levels of the organization and provide guidance and advice on compliance; report to Head on the integrity planning.

4.3 Communication and training

To develop skills and capability in integrity planning, organisations need to build a level of risk management awareness and knowledge through internal communication and training.

4.4 Positive integrity risk culture

Integrity planning is to support the development of an organisational culture where risk is appropriately identified, assessed, communicated and managed. By adopting a consistent approach to how risk is assessed, managed and communicated, a **positive risk culture** will emerge. It is one where understanding, managing and accepting appropriate integrity risk is part of the every day decision-making processes. This is in contrast to a negative risk culture where people are either risk averse, ignorant of risk or overconfident with risk taking. When an organisation maintains an integrity planning framework, it helps create an environment that is sensitive to risk taking, and eventually shapes internal attitudes towards risk.

5 INTEGRITY RISK COVERAGE: CREATING THE BASELINE TO EFFECTIVELY MANAGE RISKS

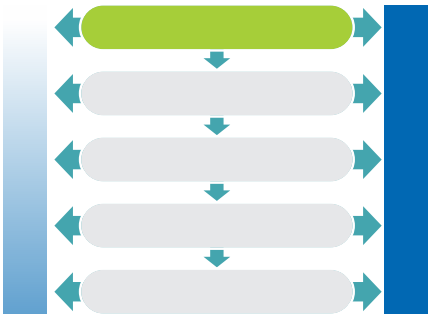
In integrity planning, organisations in Kosovo will need to address risks that are:

- **commonly present** in any organisational ethics infrastructure and are covered by the targeted anticorruption and integrity legal framework in Kosovo: such as unlawful acceptance of gifts, failure to comply with conflict of interest, failure to comply with restrictions on business, protection of whistleblowers; some common operational risks, associated with procurement, HRM and management of state property processes because of their special vulnerabilities to integrity violations;
- **institution specific risks**, stemming from their own workflow that have been identified in the course of the integrity planning process.

6 THE INTEGRITY PLANNING PROCESS

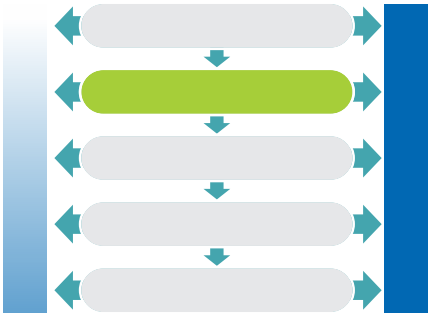
Phases	Steps	Results
Establish the context for integrity planning	**1. Review external environment** **2. Review internal environment**	**Nutshell profile** of the mandate and objectives of the public administration unit, commitment to integrity, expectations of stakeholders
Identify Integrity Risks	**3. Identify Risks and Risk Factors for each Risk**	**Relevant Risks identified, including** common and organisation specific risks
Analyze Integrity Risks	**4. Identify Controls for each Risk Factor** **5. Conduct risk analysis for every risk factor identified based on the existing treatment** **6. Assess overall risk level for each risk**	**Current treatment/ controls in place identified** for **each risk factor** Decide per **each risk factor whether it is managed, partially managed or not managed** based on the existing tretament/ controls in place The **likelihood** of an event occurring and the consequences **(impact)** if the event eventuates assessed for each risk, based on the **risk assessment matrix** relevant **risk level determined for each risk**
Evaluate Integrity Risks	**7. Rank risks and screen minor ones that donot need treatment**	**Minor risks that** don't need treatment screened, **significant risks** evaluated**, prioritised** Significant risks to be given further treatment
Determine Risk Treatment	**8. Select appropriate risk treatment/measure** **9. Prepare Integrity Action Plan/ Risk Register**	One or more **risk treatment options determined** for each risk Agree on **measures, responsibilities and deadlines**

6.1 Establish the context for integrity planning



Establishing the context for integrity planning is vital to effective integrity risk management and to intergrity planning, in particular. It provides the required understanding of the internal and external parameters to be taken into account when managing integrity risks, and sets the scope and risk criteria. The context includes both internal and external parameters relevant for the organization. *Emphasis needs to be put on integrity commitments usually codified in an Integrity Policy/ Statement*. This would require to take a closer look to the organisation, its capabilities in terms of resources and knowledge; information systems, information flows, and decision making processes; internal stakeholders; culture; standards and work models; structures (e.g. governance, roles and accountabilities).

6.2 Identify Integrity Risks



This is the process of finding, recognizing and recording risks. The purpose of risk identification is to identify what might happen or what situations might exist that may affect the achievement of the objectives of organisation. This will require to identify sources of risk, areas of impacts, events and their causes. The end results will be a comprehensive list of integrity risks based on those events that might enhance, prevent, degrade or delay the achievement of the objectives. Comprehensive identification is critical, because a risk that has been missed and has not been identified at this stage will not be included in further analysis, and therefore, never addressed.

How shall this be done? Which processes to look for?

To identify further organisation specific integrity risks, the working group shall look at the critical processes within the organisation through the following main clusters:

- ***Functions related to sectoral policy*** **- strategic planning, elaboration of draft laws, elaboration of minimal standards, indicators for assessment of sectoral policies, etc;**
- ***Operational; Delivery of services;*** **These concern the day-to-day issues that the organisation is confronted with as it strives to deliver its strategic objectives;**
- ***Regulatory functions*** **- issuing licenses, certificates, permissions, compliance checks, financial audits, etc.;**

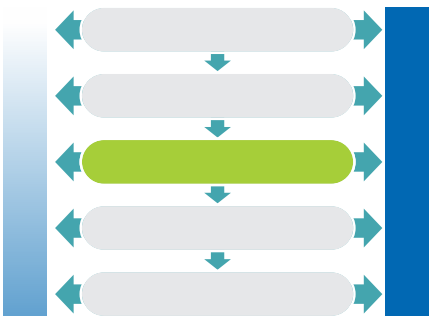
- *Functions related to coordination, supervision and control* – coordination of relationships among various bodies, supervision of the activities of subordinated structures, support to these structures in order to achieve their objectives, etc;
- *Supporting functions* – HR management, accounting, document control, IT systems, PR, organizational infrastructure, training of personnel, efficiency analysis and performance audits, maintenance of buildings/ premises, purchasing, public procurement, etc.

Identification may involve obtaining information from external sources such as monitoring reports, various other reports (audit, reports of surveillance and control authorities, inspections, regulators); criminal, civil, and regulatory complaints; administrative or judicial practice, media reports; opinion polls. This may also involve understanding the organization's processes and gathering information about potential integrity violations from *internal sources* by interviewing personnel and brainstorming with them, administering questionnaires, reviewing complaints from the whistleblower hotline, and performing analytical procedures (analyzing complaints, etc.); past practice or experience.

Valuable information may be derived from questionnaires, designed to investigate risk sensitivity of the staff and their perception of whether and how is the organisation endangered in fulfilling its objectives, as far as integrity is concerned. Fair administration of the process is a condition to its effectiveness. Experience shows that it is critical to minimise internal resistance, if any, through guaranting anonymity of the process. Results will become a valuable source of information for top management in case where a large sample is being assured. However, even a limited sample may provide with an insight as to the risk tolerance and risk taking in the organisation and may indicate particular areas of concern.

Whilst risk identification can be supported by outside consultants, an in-house approach with well communicated, consistent and coordinated processes and tools is likely to be more effective. In-house 'ownership' of the risk management process is essential.

6.3 Analyse Integrity Risks and Assess Overall Risk Level



This phase is about **getting to understand the integrity risks.** It is based on the risk identification results from the previous phase (*only identified risks and risk factors are subjected to a further analysis*) and provides an input for the next one- the risk evaluation and risk treatment phase.

Risk analysis analyzes the risks in terms of *likelihood and consequence*. This involves consideration of the current treatments/controls (actually in place) that affect the

likelihood that consequences occur, as well as an assessment of their effectiveness (whether risk factors are managed, partially managed or not managed). The working group may use various methods/ tools to analyse, evaluate risks and assess overall risk level, including but not limited to focus groups for risk evaluation, brainstorming channels, risk tables specifically designed to guide and record the assessment process. Selection of methodological tools depends on the existing capacities/ resources and needs to be aligned with the complexities/ feasibilities of the assessment. Adequate documentation is necessary.

To analyse integrity risks, the working group will need to determine the following two parameters: Likelihood of Risk Ocurring and Consequences (Impact) of Risk Occurred. There is no unique methodological solution to accomplishing this task, yet, a common method that is being used refers to the following tables.

Likelihood of Risk Ocurring

Estimation	Description	Indicators
Major /probable/	Likely to occur in **most** circumstances, known for the fact that it happens	Potential of it occurring several times within the time period (for example one year). Means that the event can happen in the next year or within the next few months and is repeated many times. Has occurred recently.
Moderate /possible/	Likely to occur in **some** circumstances- or "I have heard it has happened"	Could occur more than once within the time period (for example - three years). Could be difficult to control due to some external influences. Is there a history of occurrence?
Minor /remote/	Not likely to occur in a three year period or may occur **only under extraordinary** circumstances.	Has not occurred. Unlikely to occur unless some extraordinary circumstances appear

Consequences (Impact) of risk occurred

The severity of adverse consequences/ impacts is assessed by: the severity of the damage to the assets, operations, reputation; the scope of the damage, the approximate duration of the harmful impact; the resources needed to overcome it and recover.

Consequences (Impact)

Major	Significant impact on the organisation's strategy or operational activities; directly affects its activities, stability and assets, as well as the attainment of its objectives, Affects to a considerable degree interests of stakeholders, the society or the state; Important financial loss, mission and core activities are threatened, threat of litigation, loss of reputation and trust. Can be overcomed only in the long run with serious operational controls and considerable public resources. Practically it means that interventions in the core business and activities of the organization are necessary and a large funding to offset the damage.
Moderate	If not overcome, may lead to serious material and/or immaterial adverse impact; Moderate impact on the organisation's strategy or operational activities; Moderate financial loss Moderate stakeholder concern; can be overcomed in mid term perspective with serious control and management measures and engagement of considerable public resources. Practically it means that the consequences for the organization are rather important – and need to reorganize certain problematic activities and eliminate damage
Minor	Small financial loss, the implementation is not compromised, no judicial consequences, reputation is not jeopardized; Minor material and/or immaterial adverse impact on the organisation, that may be compensated in the short run with marginal resources by undertaking organizational and/or operational measures; Low impact on the organisation's strategy or operational activities; Low stakeholder concern; Practically no consequences - to eliminate the occurrence of an event required little action.

After determining the above two parameters *Likelihood of Risk Ocurring and Consequences (Impact) of Risk Occurred,* the working group is to determine the Risk level for all identified and assessed risk, using the Risk Matrix.

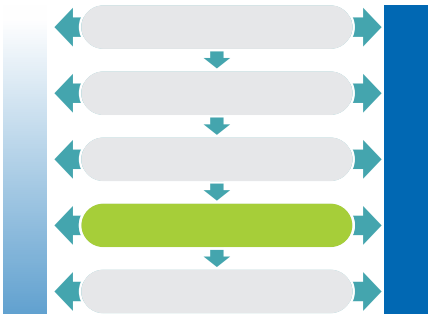
Ultimate risk level is determined, based on a Risk Matrix as a combination of likelihood and consequence.

Risk Assessment Matrix

Likelihood of risk occuring	Consequence of risk: Minor	Consequence of risk: Moderate	Consequence of risk: Major
Major	Moderate	Major	Major
Moderate	Minor	Moderate	Major
Minor	Minor	Minor	Moderate

The risk levels based on the Matrix fall under the following categories: (1) green – **minor risk,** (2) yellow- **the risk is moderate** (3) red- the risk is **major**.

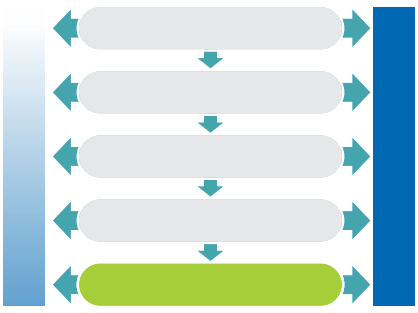
Step 4: Evaluate Integrity Risks, Set Priorities for Intervention and AC Measures



This Phase is to decide, based on the outcomes of risk analysis, about the significance of risks to the organisation and whether each specific risk should be accepted or treated to prioritize treatment implementation. Why is this important? Ideally, even minor risks may attract attention, and get treated with ongoing monitoring at least. However, organisations have limited per se resources to put in integrity management. This would require to take decisions on which risks to trate with priority.

Practically "Risk Evaluation" means to rank risks with the significant ones at the top , that account for substantial effects on organisational integrity and may endanger the efficiency, effectiveness, reliability and external image of the organisation. This should be the basis of the risk treament measures determined. Thus, priorities are set so that the available limited resources for risk treatment can go to where they are felt as most needed. Generally, risks ranked as minor, comply with the standards to risk taking and do not impose the need of extra treatment measures, but rather monitoring of the effectiveness of the treatment/ control measures in place. On the contrary, major risks requre immediate treatment with the appropriate measures.

Step 5: Determine appropriate risk treatment measures



Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once risks have been analysed, evaluated and prioritised, measures to modify the risk have to be determined and transferred to the Action Plan/Integrity Risk Register. Its purpose is to document how the chosen treatment options will be implemented. The information provided should include: proposed actions; resource requirements; and timing and schedule. This should be integrated with the management processes of the organization and discussed with appropriate stakeholders

Risk treatment itself can introduce risks. A significant risk can be the failure or ineffectiveness of the proposed risk treatment measures. This is often the case with unrealistic and overambitiuos integrity projects, the non-implementation of which results in massive lost of trust that appears hard to rebuild. Therefore, feasibility constraints, questions of phasing,

and sequencing of measures shall be taken into account in selecting the appropriate treatment. A single measure can manage one or more risk factors.

Experience shows that developing the Integrity Action Plan is sometimes neglected, meaning that limited attention is put on agreeing measures, resources, deadlines for the measures proposed. Instead, formalistic approaches often prevail, attributing deadlines and assigning responsibilities without taking into account feasibilities and priorities. Such attitudes/deficiencies minimise the chances of a targeted, feasible and timely intervention, which of itself puts at risk the effectiveness of the whole process of risk assessment. To prevent from the above, top management should pay appropriate concern to finalising the Integrity Action Plan as a basis for improvement.

Reporting of the Working Group

Integrity planning activities should be traceable. Besides tracebility and transparency, in integrity planning, records may provide the foundation for improvement in methods and tools, as well as the overall process.

Presentation of the Integrity Plan

Communication of risk exposure and risk treatment measures is important to maintain high levels of confidence from stakeholders, creating co-ownership in the improvement platform and generating support for its implementation.

Appointment of an Integrity Plan Responsible Person

The top managment nominates an Integrity Plan Responsible Person to ensure its effective implementation, monitoring and reporting.

Monitoring, Reporting and Periodic Re-assessment and Review

Monitoring

Organisations are dynamic themselves and operate in a dynamic environment. Therefore, the ongoing monitoring of implementation of Integrity Plans is critical to ensure that the integrity risk control and treatment measures are effective in both design and operation; that procedures are understood and the integrity plan followed. Further to that, monitoring should also:

- **determine whether the risk treatment measures adopted produced the planned effects;**
- **detect changes in the external and internal context including changes to the risk itself which can require revision of risk treatments and priorities;**
- **identify what lessons could be learned for future assessments**

Reporting

Regular reporting is essential to ensure that the implementation of the integrity planning is following the schedule and planned results are being achieved. The Integrity Plan Responsible Person, shall therefore, periodically report to the top management on the implementation of the Integrity Plan measures within planned intervals. Reporting allows the organisation to undertake on time adequate corrective/ preventive measures in case where implementation of particular measure(s) poses difficulties/ delays.

Re-assessment

Since risks and threats change over time, it is important that institutions periodically reassess risks and reconsider the appropriateness and effectiveness of the risk management policies and controls they have selected. Changes in the organisation and the environment in which it operates must be identified and appropriate modifications made to systems. The re-assessment process shall build on the results and experience of the previous ones, considering the lessons learnt from the implementation so far, the results of the regular compliance and performance audits should be reviewed to identify opportunities for improvement.

Finally, it is the continuous improvement cycle that drives improvements in all organisational management processes, the integrity management included. Therefore, integrity planning is not to be considered and implemented as an one-time accidental exercise, legally and strategically required, but undertaken with a view that it may be the first, but definitely not the last step in the organisational integrity management. Although the first steps may be difficult as understanding and experise are still to mature, continuous effort will eventually turn the assessment and planning exercise into a routine practice that becomes an integral part of the organisational management. Viewed from the perspective of organisational learning, it is not that much the end result (i.e. the individual Integrity Plan developed), but rather the process of integrity planning that may cause a change. It builds a sensitive and determined risk taking, that allows stakeholders to face risks with no reservations, but shared beliefs that minimized opportunities and raised incentives to combat corruption will necessarily produce results and help the organisation achieve its objectives and be trusted by stakeholders.

7 INTEGRITY MANAGEMENT MODEL

7.1 Why system approach to prevent corruption and safeguard integrity

Integrity Management, as opposed to corruption control or integrity assurance, most accurately reflects the all encompassing importance of integrity throughout all the organization's operations. It represents the organisational ability to fulfill in practice its commitment to a an integrity policy and code of conduct on behalf of all its stakeholders.

7.2 Integrity Management System

A set of interrelated components and their interactions developed, maintained, monitored and improved as a practical system for preventing, detecting and sanctioning corrupt practices. It is what the organisation does to ensure that its operations are corruption free.

7.3 Goal

The goal is to ensure ethical delivery and adherence to integrity in all activities, i.e. provided services.

7.4 Components

- Integrity policy and Code of Conduct
- The organizational structure: allocation of roles and responsibilities
- Training programmes and awareness raising
- Communication with internal and external stakeholders
- Integrity risk assessment/ Integrity Plan
- Integrity controls and procedures for all key processes
- Integrity audits
- Monitoring and investigation of corruption related cases
- Reporting as regards integrity performance
- Integrity management reviews

7.5 Principles

Leadership: Top management must clearly and visibly demonstrate an active, evidence based commitment to integrity. This would require them to lead the process since the very beginning, through developing the integrity policy and the Code of Conduct. Critically important is this commitment to be continuous, and that it is well understood and well seen by all stakeholders, internal and external.

Involvement of staff: Every employee's participation is critical to the successful implementation of the integrity management system. Meaningful involvement, however, requires appropriate education and training in integrity related issues, structured awareness raising generating trust and a positive environment within which to work. A working environment committed to integrity empowers staff. Effective internal and external communication and coordination is vital to successful teamwork so that all the parties involved obtain and maintain the same understanding of the project while it is being carried out.

A System Approach: Identifying potential areas of corruption and managing interrelated processes to ensure integrity requires a systems approach. This will need organisations to pay attention to all components of the system and analyse the relationships and interdependencies between them.

7.6 How to develop an integrity management system

Any organisation that serves its mandate and strives to achieve its organisational objectives, in one way or another exibits one, some or more elements of a model integrity management system. Thus, some organisations have formulated anticorruption policies; developed integrity programmes or ethics compliance programmes; appointed ethics counsellors; introduced integrity audits; implement anticorruption awareness and capacity building plans; installed anticorruption hotline to report corruption; report to external stakeholders abour corruption cases; set up investigation and enforcement teams to maintain the zero tolerance to corruption policies, etc. Some organisations implement part of the above measures; others most of them. To sustain a function integrity management system, however, requires organisations to implement a fully pledged Plan - Do - Check - Act (PDCA) continual improvement framework and incorporate integrity management into everyday organizational practices. In other terms, it requires that the organisation to (1) **plan** its integrity related policies, code of ethics and integrrity plans;(2) implement the integrity management action plans;(3) **check:** monitor and measure key characteristics of operations that determine organizational performance as regards prevention of corruption and integrity against the integrity policy and objectives, and report the results; and (4) **take actions** to continually improve organizational performance as regards prevention of corruption and integrity and the integrity management system. To this purpose, the following practices may be considered.

7.7 Managing Integrity - Good Practice Guide for Public Sector Organisations

Integrity must be reinforced **at every step and by everyone.** Good practices for ensuring effective internal controls, ethics, and compliance programmes or measures for the purpose of preventing corruption and safeguarding integrity are listed below:

Explicit and visible support and commitment from top management to the code of ethics, compliance programmes, internal controls and other measures for preventing corruption and safeguarding integrity. Management has overall responsibility for the design and implementation of effective integrity risk management program. **Management is to create a culture through words that are understood and actions that are visible,** making it clear that corruption is not tolerated, that any integrity violation is dealt with decisively, and that whistleblowers will not suffer retribution.

A clearly articulated and visible integrity policy to reinstate the commitment to integrity and to convey the expectations of the top management as regards the integrity performance of the organisation, including compliance with legal requirements and Code of ethics. The integrity policy should be documented, implemented, communicated internally and externally, and be made publicly availableCode of conduct to ensure adherence to values and commitment, To support understanding, code should be clear, simple and easy to communicate and apply.

Roles and responsibilities

An effective integrity risk management presupposes a clear division of the roles and responsibilities that staff at all levels of the organization has with respect to integrity management. Policies, charts, job descriptions, should unambugiously define roles and responsibilities related to integrity risk management.

Appointment of an Integrity Officer (Counsellor, Guardian) or Integrity commitee

As part of the integrity management system, a senior member of the staff should be appointed as the one responsible for the governance oversight of integrity control to assure that procedures are implemented and allow for effective communication between top management and staff on integrity related issues.

Staff

Strong controls against corruption are the responsibility of everyone in the organization. All levels of staff, including management, should:

» Have a **general understanding of the conceptual framework** as regards integrity and corruption and be aware of the concrete forms of corruption and the red flags.
» **Understand their roles within the internal control framework,** how their job procedures are designed to manage integrity risks and when noncompliance may create an opportunity for corruption to occur or go undetected.
» **Understand and implement policies and procedures** (e.g. the integrity policy, code of conduct), as well as other operational procedures
» As required, participate in the process of creating a strong control environment and designing and implementing integrity control activities, as well as participate in monitoring activities, including reporting suspicions or incidences of corruption.
» Cooperate in investigations.

Conflict Disclosure

The organisation should implement a process for management, staff and contractors to disclose potential or actual conflicts of interest.

Effective internal communication as regards corruption and integrity across functions and levels within the organisation. This could include measures for: providing guidance to staff on complying with the ethics and compliance programme; internal and confidential reporting by, and protection of all staff, and, where appropriate, business partners, willing to report breaches of the law or professional standards or ethics occurring, in good faith and on reasonable grounds; and undertaking appropriate action in response to such reports.

Protection of whistleblowers through sustaining a system that enables confidential reporting of integrity violations, including breaches of the law or professional standards or ethics occurring within organization, in good faith and on reasonable grounds by internal and external interested parties; as well as through undertaking appropriate follow up action in response to such reports.

External communication with stakeholders

Informing stakeholders of the commitment to abiding by anticorruption laws and standards, and of the integrity policy and ethics and compliance programme and measures for preventing corruption; and seeking a reciprocal commitment from partners. It is also critical that the organisation obtains external or client/ beneficiary/partner feedback. Various channels may be used: anticorruption hotline, client evaluations: solicited in a number of ways, including a direct inquiry asking for comments on specific issues, or through an easy-to-complete questionnaire; conducting follow-up debriefings on proposals, won or lost, and on completed assignments; commissioning an external audit, to obtain an independent evaluation of the integrity management system; peer review or risk assessment, to assist the organisation in identifying areas that require further attention.

Training for all staff, on the ethics and compliance programme or measures regarding corruption and integrity. This may include receiving an initial orientation and ongoing education on the integrity risk management measures in place, including the codes of conduct and ethics, what constitutes fraud, and what to do when fraud is suspected. The effectiveness of this training is dependent on the periodic updates and level of commitment demonstrated.

Awareness raising measures, where appropriate, to encourage and provide positive support for the observance of ethics and compliance programmes or measures against corruption, at all levels;

Integrity risk assessment and integrity plans/ethics and compliance prgrammes

To protect itself and its stakeholders effectively and efficiently from corruption, the organisation shall understand integrity risks inherent in its activities and implement integrity planning. The assessment shall be integrated with an overall organizational risk assessment and should, at a minimum, include risk identification, risk likelihood and significance assessment, and risk response. The integrity plan is the basis for improvement of the organisational resistance to corruption and results of integrity assessments will need to be considered when determining controls.

Establishing Enforcement Measures

The organisation shall determine those operations and activities that are associated with the identified integrity risk(s) where the implementation of controls is necessary to manage the integrity risk(s). For those operations and activities, the organization shall implement and maintain: operational controls, as applicable to the organization and its activities; the organization shall integrate those operational controls into its overall integrity management system; controls related to contractors and other visitors to the workplace; documented procedures, to cover situations where their absence could lead to deviations from the integrity policy and objectives.

Monitoring the Integrity Management Process

Implementation of an integrity management system requires continuous monitoring of activities and service delivery to make sure that there is compliance.

Integrity audits

The organisation should periodically plan conduct internal audits to determine whether the integrity management system conforms to planned arrangements for integrity management; and whether it is effectively implemented and maintained. The selection of auditors and conduct of audits shall ensure objectivity, impartiality and confidentiality of the audit process.

Investigation of integrity violations

No system of internal control can provide absolute assurance against corruption and integrity violations. Thus, top management should ensure the organisation develops a system for prompt, competent, and confidential review, investigation, and resolution of instances of noncompliance and allegations involving potential integrity violations.

Appropriate disciplinary procedures to address, among other things, violations, at all levels of the organisation, of anticorruption laws, and the ethics and compliance programme.

Corrective Action

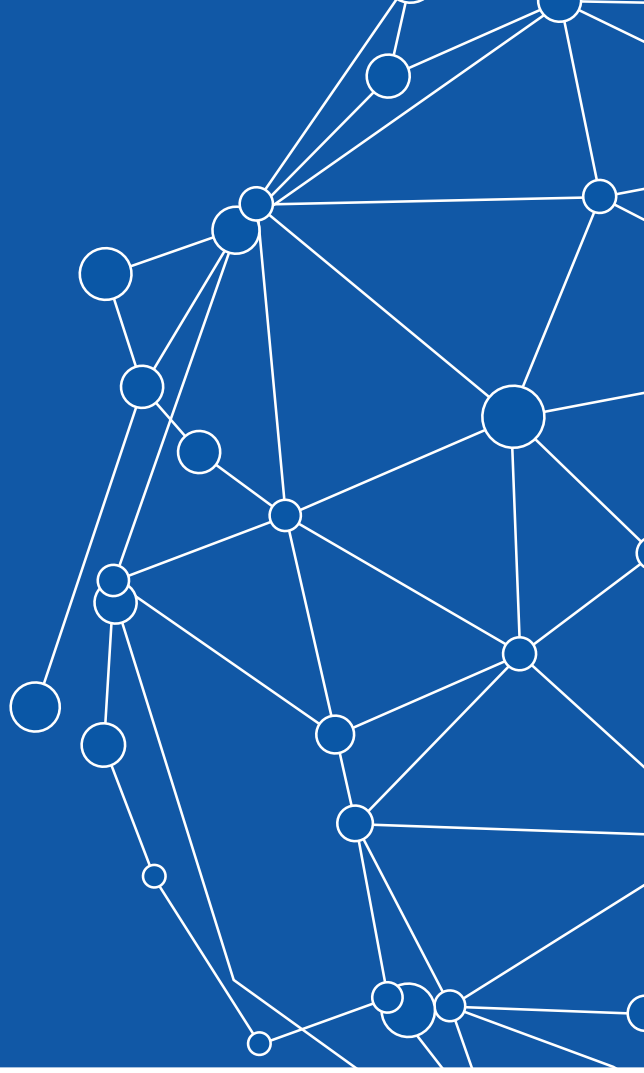
If specific components of the integrity management system are not met, the organisation will have to establish corrective action promptly in accordance with the relevant legal rules, to address the deficiencies.

Management review of integrity performance and the functioning of the integrity management system: Systematic and periodical review to analyze and review the integrity management system functions and the integrity performance of the organisation should be in place. It is to assure its continued suitability and effectiveness, and ensure that the organisation responds adequately to the to-date challenges of the corruption and integrity risks. This will include a review of the integrity policy; the results of participation and consultation; the integrity performance of the organisation; the implementation of the integrity plan/measures, to evaluate their effectiveness in preventing and detecting corruption, and decide on improvements considering relevant new developments and evolving international and sector standards.

8 BIBLIOGRAPHY

STANDARDS AND OTHER PUBLICATIONS

- ISO/IEK 31010, Risk management- Risk Assessment Techniques
- ISO Guide 73:2009 Risk management- Vocabilary
- ISO 31000:2009 Risk management- Principles and guidelines
- BS 10500 Specification for an anti bribery management system
- Australian/New Zealand Standard for anti corruption - AS 8001-2008 Fraud and corruption control
- ISO 26000 Guidance on social responsibility
- BS EN ISO 9001:2008, Quality management systems – Requirements
- BS ISO/IEC 20000, Information technology – Service management
- BS ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements
- Federation of European Risk Management Associations (FERMA) Risk Management Standard, available at http://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-english-version.pdf
- Association of Insurance and Risk Managers (AIRMIC), Public sector risk management association (Alarm) and Institute of Risk Management (IRM)- A Guide to ISO 31000, available at http://www.ferma.eu/app/uploads/2011/10/a-structured-approach-to-erm.pdf
- Committee of Sponsoring Organizations of the Treadway Commission (COSO)- Enterprise Risk Management (ERM) standard 2004
- Federation of Consulting Engineers (FIDIC) Integrity Management System (FIMS) Guidelines: 2011, available at http://fidic.org/books/integrity-management-system-fims-guidelines-1st-ed-2011-part1
- A Guide for Anticorruption Risk Assessment, UN Global Compact, 2013, available at
- https://www.unglobalcompact.org/resources/411
- Business Principles for Countering Bribery and associated tools. Berlin: Transparency International. 2009.
- PAS 1998, Whistleblowing arrangements – Code of Practice (freely available as a download from www.pcaw.co.uk/bsi or www.bsigroup.com/PAS1998)
- United Nations Convention against Corruption. New York. 2004
- Convention on the Bribery of Foreign Public Officials in International Business Transactions and Related. Documents. Paris: OECD. 2010.
- The Bribery Act UK 2010. Chapter 23. London: TSO.
- [The Bribery Act 2010: Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing (section 9 of the Bribery Act 2010). London: Ministry of Justice. 2011.
- Good Practice Guidance on Internal Controls, Ethics, and Compliance. Paris: OECD.
- 2010. available at http://www.oecd.org/investment/anti-bribery/anti-briberyconvention/44884389.pdf
- Combating Extortion and Bribery: ICC Rules of Conduct and Recommendations. Paris: ICC. 2005.
- Business Integrity and Transparency Principles for the Private Sector. Singapore: Asia-Pacific Economic Cooperation (APEC) 2004



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Cooperation Office Kosovo

UNDP

Empowered lives.
Resilient nations.