Integrity Assessment of Public Sector Organisations

MANUAL

Integrity Audit

2014

Contents

Introduction

This manual consists of two parts:

Part I	Principles of the methodology
Part II	Guidance for application

Preface

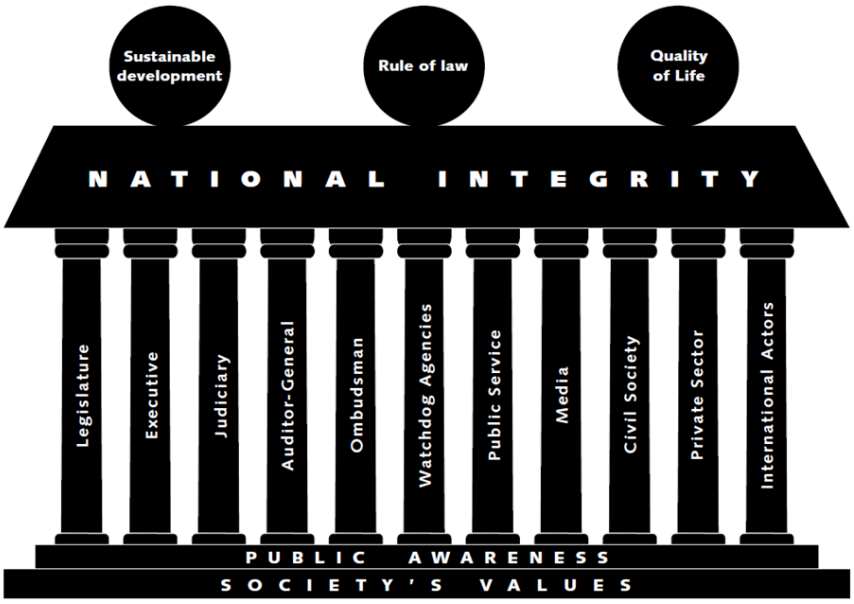
Supreme Audit Institutions have an important role to play in safeguarding the integrity of the public sector. Traditionally their role is to audit the execution of the State budget, public spending and management of public property. In this way SAIs contribute to a good management of public money and are an important 'pillar' in what Transparency International calls 'the National Integrity System'. But SAIs are also expected to specifically contribute to combating fraud and corruption. There are different ways this can be done and the appropriate strategy depends on the specific circumstances in each country.
Traditionally the first resort in the fight against corruption is repression. This means a rule based approach that is focused on legislation, detection and prosecution of corruption. This can be focussed either on people (detection, investigation and prosecution) or on the system (legislation and compliance). However, there is more and more recognition of the fact that such a single handed approach is not enough, and can sometimes even be counterproductive. Enhancing the integrity of public sector organisations can offer a powerful complementary approach. It draws the attention to alternative values of ethics and integrity to replace a habit of corruption, thus opening up possibilities to replace unwanted behaviour of corruption by proposing desirable behaviour of integrity. This can be focussed either on people (culture, civil society) or on the system or organisations (management). This strategy is preventive; principle based and empowers the management and employees of public sector organisations and civil society in the fight against corruption.

This guideline is meant to give SAIs guidance on how to conduct an audit on the integrity management of public sector entities. It is in line with ISSAI 5700 (Guideline for the audit of Corruption Prevention in Government Agencies), but will provide more detailed guidance and tools.

1 National Integrity System

UNCAC has described the government wide system of coordinated anti-corruption policies, also referred to as the 'National Integrity System' (NIS). This system has the purpose to provide the necessary 'checks and balances' through a dispersion of power between the different agencies and branches of the public sector, and between the public sector and civil society. The complete NIS framework can be illustrated as a Greek temple, as shown in figure 1.2.

Figure 1.2 The National Integrity System (NIS)



1 Source:

2 Pope, Jeremy, 2000. Confronting Corruption: The Elements of a National Integrity System, TI Source Book 2000, Transparency International, p. 35.

As the figure illustrates, NIS also consists of a foundation comprising 'public awareness' and 'society's values', and, on the roof, 'sustainable development', 'rule of law' and 'quality of life'. The last three elements are depicted as round balls to make it clear that the roof must be kept level to prevent them from rolling off and being destroyed. Equally important as the 'temple' and the institutional pillars, however, are the rules and rules and practices for the functioning of these pillars and the integrity system[1]. As effective anti-corruption policies in society depend on a well-functioning NIS, these pillars and rules and practices are also to a large extent recognized in UNCAC.

[1] AFROSAI-E *Preventing and detecting Fraud and Corruption* 2014

2 Assessment of integrity management in the public sector

To assess the maturity of the integrity management of the public service(s) in a country there are several audit options. The goal is to identify weak organizations or departments within the public service.

2.1 Base line measurement

A base line measurement is a government wide inventory and analysis of laws and regulations that may serve to support and shape the integrity of the public sector in a country[2]. It seeks to answer three basic questions:

1. To what extent has the requirement of good governance been further developed in terms of regulations relating to the management of integrity?
2. To what extent has government complied with the requirements (as stipulated by law) to further develop certain aspects of integrity, to develop (integrity) norms in national decrees containing general measures, and to issue ministerial regulations etc.?
3. To what extent are the regulations containing aspects of integrity and which dictate rules for implementation actually executed and enforced?

To answer these questions, typically an inventory of all published laws (national ordinances) related to (aspects) of integrity is made. In addition, an inventory (catalogue) can be made of all articles (of national ordinances) that require further implementation rules and norms.
Then a review is done to determine which of the implementation rules/regulations are actually present and whether these are functioning.

2.2 Audit of Integrity Management

Every public sector organisation faces integrity risks to a greater or lesser degree. It follows that each organisation must take measures to prevent unethical conduct. It is important in this connection to have a balanced package of measures designed to prevent, detect and repress breaches of ethical conduct. Such a package is known as an integrity management system.

[2] General Audit Chamber St Maarten: Baseline study Institutional integrity Management 2014

Typically there are two main approaches: a repressive rule based approach and a stimulating principle based approach. A well-balanced mix of both approaches is necessary for good results. The audit of integrity management focuses on whether an public sector organisation has implemented an adequate set of integrity measures to control its integrity risks that might seriously undermine confidence in the organisation and thus in its image and continuity.

The basic audit framework for the audit of integrity management consists of 6 main components[3]. For each of these components audit criteria need to be determined, depending on the scope of the audit and the specific national legislation and vulnerabilities of the audited entity. The components are:

1. A public sector entity must be incorruptible and dependable
2. A public sector entity must have a sound analysis of its integrity risks
3. A public sector entity should have implemented a relevant set of measures to prevent integrity incidents
4. A public sector entity should have a relevant set of measures implemented to follow-up and mitigate damage of integrity incidents
5. A public sector entity must regularly evaluate its integrity policy
6. Compliance of the public sector entity's integrity policy should be subject to internal and/or external audit

2.3 Regularity and efficiency audit of the ethical infrastructure in public sector organizations

The main objective of auditing the regularity and efficiency of the ethical infrastructure in public sector organizations[4] is to evaluate regularity and efficiency of functioning of ethical infrastructure and to assess ethical conduct of civil servants and compliance with ethical values and principles.

Besides main audit objectives, there are also specific audit objectives to check and assess: completeness of ethical infrastructure in the public sector, implementation of rules and regulations related to ethics, level of ethical infrastructure establishment and efficiency of its implementation, level of relevant knowledge and skills of civil servants, treatment of complaints, cooperation with other subjects and importance of ethics in the government bodies.

---

[3] Netherlands Court of Audit *Integrity Management: A Government wide measurement of integrity management in 2004 and 2009*

[4] SAI Croatia *Regularity and efficiency of the ethical infrastructure functioning in the government bodies*

The purpose of establishing the ethical infrastructure is assuring, through the use of efficient mechanisms, the application of ethical principles, the following of fundamental ethical values, monitoring their application and undertaking the appropriate measures, procedures and sanctions in the cases of unethical behavior.

2.4 Transversal audit of integrity management in the government

A transversal audit can be defined as the simultaneous examination whereby cross-cutting issues such as a specific focus area, theme or topic is examined in more than one audited entity using the same audit methodology and procedures[5]. The audited entities could be Ministries, Departments or Agencies (MDAs). Transversal audits maybe referred to as government-wide, horizontal, or theme audits and they can have a regularity or performance audit focus or a combination of both.

Benefits of transversal audits include the following among others;

- It is an approach which allows the identification of specific problems across government or affected entities, including weaknesses in controls and systems and training needs;
- Assisting government prioritization process by offering government wide solutions to identified problem areas.
- Dictates a consistent audit approach is followed for a specific area;
- Enables the identification of gaps in legislation and policies;
- Allows SAIs to link to government initiatives and aspects deemed to have great importance by Parliament and other stakeholders. This increases the ability of auditors to provide relevant information, advice and assurance;

2.5 Focus of this manual

The first type of audit (base-line measurement) may be a good starting point if there has been no evaluation yet of the legislation that support the National Integrity System. In most countries it is the OECD, Transparency International or the UN that usually provides this type of assessment or (peer) review. Of course the SAI can also be in the position to do such an analysis.

The second type of audit (audit of integrity management) is the object of this manual. This type of audit can be also applied in the audit of ethical infrastructure and transversal audit. Both these types are a mix of integrity audit and performance audit. All kinds of varieties are

[5] AFROSAI-E *Preventing and detecting Fraud and Corruption* 2014

possible, but this manual focusses on the audit of integrity management, because this is the basic approach a SAI can adapt to its own purposes.

Part II: Guidance for application

3 Assessment of the "maturity level" of the integrity control system

The assessment of the maturity level of the integrity control system takes into account the existence, the operation and the performance of controls. This makes it possible to analyse the strengths and weaknesses of the integrity control system. In this way it provides an insight into the resilience the organisation has already built up to integrity violations. In an ideal situation, the maturity level is based on:

- the presence of measures;
- the quality and suitability of the measures and their design;
- communication of the measures and the staff's awareness of them;
- the acceptance of the measures;
- the embedding of the measures in the planning & control cycle;
- the quality of the measures' implementation and enforcement;
- the supply of information and accountability for the implementation and effect of the measures;
- the evaluation and, where necessary, revision of the measures.

3.1 How to set the framework

The principles and standards to use in assessing and auditing the integrity management systems consist of different types of norms. First, there is the legal framework. The legal framework consists of international regulations and national laws that can differ from country to country. Then there is the institutional framework. Rules and regulations that organizations set to prevent fraud, corruption and other integrity breaches. And last but not least there are the internal controls of organizations to enhance moral conscious behaviour and stimulate rule following.

In this chapter several levels of control measures are presented. The framework for the assessment of the integrity control system of the audited entity differs from audit to audit and from audit object to audit object. It consists of several types of controls, which ones depends on the legal framework in the country, on the national integrity system, on the assessment of the integrity management in the public sector, on the institutional framework and on the outcome of the assessment of integrity risks and vulnerabilities of the audit object.

3.2 Legal framework

The existence of ethical guidelines/Codes of Conduct and other administrative guidelines are important to address conflicts of interests and prevent fraud and corruption in the Legislative, Judicial and Executive branches of government, as well as in the Auditor General's office. However, to provide for effective deterrence – and hence prevention – of more serious cases of fraud and corruption, sanctioning through criminal and administrative law is also required. UNCAC prescribes that State Parties adopt measures through legislation and otherwise to criminalize several acts. Moreover, in addition to the aspect of criminalization, it also provides provisions in relation to law enforcement, which are equally important from a sanctioning perspective. The articles on law enforcement also includes provisions on the protection of witnesses and 'whistleblowers', i.e. people who report cases of fraud and corruption, mismanagement and other illicit or improper conduct[6].
Every country has its own national legal framework, because of that in this manual there is no extensive description of the national legal framework.

It is helpful to have had a baseline study with an inventory of all the laws and regulations in one's country to audit the quality of its legal framework with respect to integrity. Have all the main issues been covered? Did the government comply with all the requirements stipulated by law? See for example in Annex 3 the audit of the Audit Chamber of Sint Maarten on integrity: Baseline Study Sint Maarten. State of affairs institutional integrity management 2014.

3.3 Institutional framework

Organisations should have integrity policies and codes of conduct based at least in part on specific risk analyses. The policies and codes should contain the compulsory elements arising from primary and secondary legislation. Management and personnel should be actively involved in the formulation of policy and the conduct of risk analyses, in part because of their ability to identify risks and dilemmas. The code of conduct should act as a standard: its rules should be formulated so as to make clear what behaviour is required and explain what sanctions will be imposed.

3.4 Internal control measures

COSO has established a common internal control model against which companies and organizations may assess their control systems. COSO is a joint initiative of five private

[6] AFROSAI-E *Preventing and detecting Fraud and Corruption* 2014

sector organizations, established in the United States, dedicated to providing thought leadership to executive management and governance entities on critical aspects of organizational governance, business ethics, internal control, enterprise risk management, fraud, and financial reporting[7].

Definition of "Internal Control" in INTOSAI GOV 9100:
"Internal control is an integral process that is effected by an entity's management and personnel and is designed to address risks and to provide reasonable assurance that in pursuit of the entity's mission, the following general objectives are being achieved:

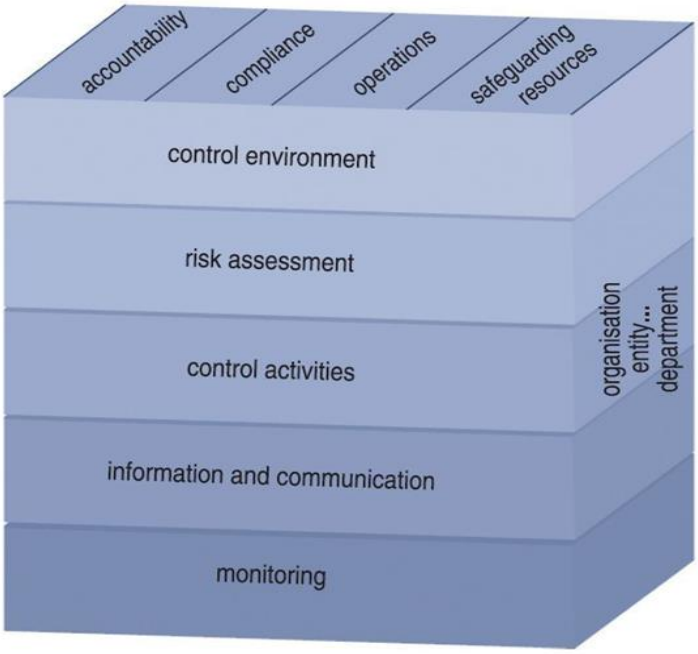
- executing orderly, ethical, economical, efficient and effective operations;
- fulfilling accountability obligations;
- complying with applicable laws and regulations;
- safeguarding resources against loss, misuse and damage."

The COSO framework defines internal control as a process, affected by an entity's board of directors, management and other personnel, designed to provide "reasonable assurance" regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations.
- Safeguarding of Assets (MHA)

Figure 3.1 COSO - Control 'cube'

[7] AFROSAI-E *Preventing and detecting Fraud and Corruption* 2014



Source: COSO

The COSO internal control framework consists of five interrelated components derived from the way management runs a business.

Control environment: The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, management's operating style, delegation of authority systems, as well as the processes for managing and developing people in the organization.

Risk assessment: Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives and thus risk assessment is the identification and analysis of relevant risks to the achievement of assigned objectives. Risk assessment is a prerequisite for determining how the risks should be managed.

Control activities: Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address the risks that may hinder the achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

Information and communication: Information systems play a key role in internal control systems as they produce reports, including operational, financial and

compliance-related information, information that makes it possible to run and control the business. In a broader sense, effective communication must ensure information flows down, across and up the organization. For example, formalized procedures exist for people to report suspected fraud. Effective communication should also be ensured with external parties, such as customers, suppliers, regulators and shareholders about related policy positions.

Monitoring: Internal control systems need to be monitored; it is a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities or separate evaluations. Internal control deficiencies detected through these monitoring activities should be reported upstream and corrective actions should be taken to ensure continuous improvement of the system.

The following principles and standards form the basis of integrity management systems[8]:

- The integrity policy should be periodically evaluated. Where necessary, the organisation should adapt the policy in response to the evaluation results.
- Internal controls should be in place specifically for compliance with the integrity policy and the code of conduct. The effect of these internal controls should be monitored and reported to management.
- The organisation's external auditor or internal audit department (AD) should audit compliance with the integrity policy. The audits should lead to conclusions and recommendations and the organisation should learn from the audit findings.
- The organisation should keep an orderly and up-to-date central record of reports of possible or actual unethical conduct. The reports should be investigated and assessed. Possible or actual violations should also be analysed as to their scope, prevalence, size and causes. The organisation should learn from the incidents.
- If there is a concrete suspicion of an offence, the organisation's management should report it to the Public Prosecution Service.
- Sanctions (disciplinary action) should be applied in accordance with the applicable criteria (based on the integrity policy or code of conduct).
- If integrity provisions are to be effective, the staff of the organization concerned must be familiar with them and the rules must actually be applied.

[8] Netherlands Court of Audit *Integrity Management: A base-line measurement of integrity management in 2004*

3.5 Hard controls and soft controls

Internal control involves human action, which introduces the possibility of errors in processing or judgment. Internal control can also be overridden by collusion among employees or coercion by top management.

There are two types of ethical behaviour[9]: following rules and moral conscious behaviour. Hard controls and soft controls can be used to enhance following rules and moral conscious behaviour. Soft controls are aimed at awareness and the moral competence of employees. There are five hard and soft controls that have shown to be contributing to following rules and moral conscious behaviour:

- Organisational policy on integrity
- Tone at the top
- Values and norms
- Fairness of treatment
- Relationships among colleagues

Organisational policy on integrity

There are two dimensions in integrity policy: rule based and principle based. The rule based policy is repressive and legalistic. It focuses on determent of bad behaviour by detection and punishment. It needs clear rules and independent execution in order to maintain rule of law and fairness. The principle based policy is an approach that is focused on facilitating good behaviour and rooted in stimulating an ethical culture. It needs a wide definition of integrity. For example: formulating a code of conduct alone is not enough. Employees need to know and understand the policy to make it work.

Tone at the top

The example that managers and leaders of organisations set for their staff is the most influential factor on the integrity of the organisation. Not only should they reflect ethical standards in their own behavior, but also stress the importance of ethics and integrity, e.g. by taking integrity management seriously, being transparent and true to their word and responding directly to incidents.

Values and norms

Setting values and norms is an important instrument for strengthening the integrity of an organisation. Acting with integrity is not just the responsibility of each individual employee, but also of the organisation as a whole. The organisation is responsible for

[9] EUROSAI Taskforce on Audit & Ethics *SUPPORTING SAIs TO ENHANCE THEIR ETHICAL INFRASTRUCTURE , Part II: Managing Ethics in Practice- analysis,* 2014

providing a safe working environment in which employees are protected as far as possible from integrity risks.

Fairness of treatment

When the intention behind rules and regulations is not understood by the target audience, it is very difficult for them to comply. Also, it is important that the rules are carried out in a responsible matter. Even people who didn't want to break the law might find themselves doing so as soon as they feel that rules are not fairly executed. There needs to be room for personal development within the SAI. This also means that there is room to make mistakes and to learn from them.
The SAI should not tolerate any form of discrimination.

Relationships among colleagues

Relationships among colleagues play an important role to success in the workplace. A pleasant working atmosphere is essential for a good performing organisation. This means being open in our communication, working together well and helping each other. That also helps to promote an ethical attitude towards work. When employees get along they are more likely to discuss ethical dilemmas and ask each other for advice.

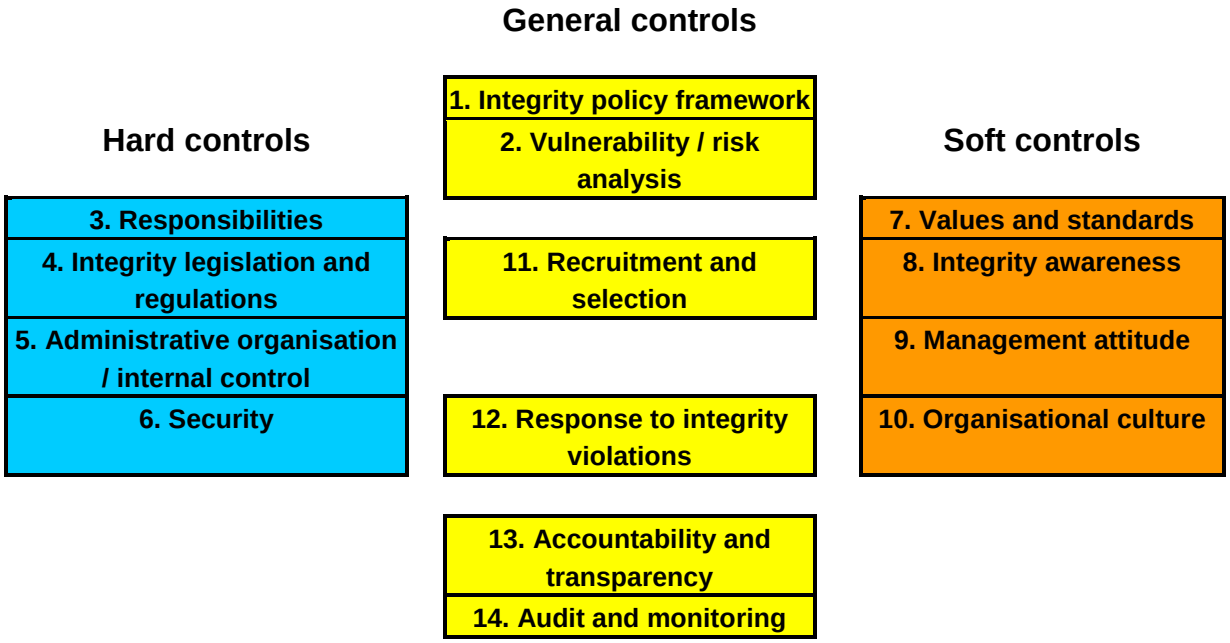
3.6 IntoSAINT framework of controls

A detailed and extensive set of integrity controls is provided by IntoSAINT. A key element of this methodology is the assessment of the "maturity level" of the integrity control system. The integrity control system is the body of measures in place to promote, monitor and maintain integrity (cf Coso). From the many measures known from the literature and practice a keenly-balanced set has been composed to serve as reference for this assessment method.

The institutional framework for the audit can be taken from this extensive set, taking into account the organisational integrity risks and the legal requirements.

The assessment of the maturity level of the integrity control system takes into account the existence, the operation and the performance of these controls. This makes it possible to analyse the strengths and weaknesses of the integrity control system. In this way it provides an insight into the resilience the organisation has already built up to integrity violations.

IntoSAINT provides an extensive set of integrity measures divided into three main groups (general, hard and soft controls) and 14 clusters of hard, general and soft controls.
The clusters are shown in the model below.



A complete list of all measures is also provided in the annex 2 of this manual.

4 Design and execution of the Audit

Once the framework has been established the audit must be designed and planned. What data and information are needed to answer the audit questions and formulate an opinion on the maturity of the integrity management? How can we manage the expectations of the public and communication with the auditees? How do we make sure the audit has the desired effect, i.e. to improve the integrity of our public sector organisations? In this chapter we give some guidance on these issues.

4.1 Gathering data

Like there is in regularity and performance audits, there are a lot of different ways to gather information and evidence to execute your audit. To gather your findings you can choose from the following methods:

- Meetings / interviews with representatives of the audited entity (ethics commissioners and management) [10]
- The analysis of relevant documentation (internal regulations, procedures, Ethical Commissioner's records and reports) [18]
- A questionnaire for civil servants + statistical analysis of replies[18]
- Accountant reports, Internal reports
- Registers of new organisations and public private organisations
- Analysis of legislation,
- client satisfaction,
- Complaints (e.g Ombudsman)
- Interviews
- Employee perception
- Analysis of old cases
- Network politician and organisation
- Newspaper clippings
- Lack of Resources: Study of budget cutback, actual mandate and budget
- Monitoring and review of the work of audited entities18
- Benchmarking[18]
- Voluntary based data collecting (personal anonymity)[11]
- Employee satisfactory studies[12]
- Shadow business (mystery guest)[20]
- Situation analysis (how should it be compared to the reality now)[20]
- Previous audit information[20]

---

[10] SAI Croatia *Regularity and efficiency of the ethical infrastructure functioning in the government bodies*

[11] State Audit office of Hungary *Integrity: A project to strengthen the integrity-based administrative culture in Hungary* , 2013:

[12] EUROSAI Taskforce on Audit & Ethics *Seminar on Auditing Ethics: workshop Assessment INTegrity*, 2013

- Whistle blower information[20]
- Analyzing the cultural framework[20]
- Comparing to good practices[20]

4.2 Gap analysis

After completing the assessment of vulnerabilities and the maturity level of the integrity control system, it becomes possible to analyse whether the existing system of controls is more or less in balance with the level of vulnerability of the organisation and its processes. If both levels are not in balance, there is a gap, usually indicating that the integrity control system needs strengthening[13].
The gap analysis may be conducted on two aggregation levels:

- Level 1: on the level of the entire organisation the integrity control system as a whole should be in balance with the vulnerability level of the organisation;
- Level 2: on the more detailed level of specific risks or procedures the maturity of mitigating controls should be sufficient.

Organisations may cope with vulnerabilities in different ways. First of all they may try to eliminate or reduce vulnerabilities by avoiding vulnerable activities. Sometimes it is possible to conduct activities in a different way thereby eliminating activities that are vulnerable to breaches of integrity. This means that the organisation is able to address the origin of the vulnerability. In practice however this may be difficult. Public organisations have legal obligations and cannot avoid engaging into sensitive activities.

Usually a more viable way to cope with vulnerability is to design and implement compensating (integrity) controls. Depending on the 'maturity level' of the integrity control system the organisation is more or less resilient to the vulnerabilities it is facing.

4.3 Reporting

The audit report should focus on the gap analysis, because this analysis shows the level of the remaining vulnerability of the organisation and should be the basis for the recommendations.

There are two types of recommendations possible, based on the assessment:

- recommendations aiming at reducing vulnerabilities and vulnerability enhancing factors;
- recommendations, aiming at improving integrity controls.

[13] Netherlands Court od Audit *Manual IntoSAINT Integrity Self Assessment for Supreme Audit Institutions*, 2011

Recommendations given on the basis of the particular facts and findings of the audit, but also the simple fact that the audit was conducted, are able to produce the following types of improvements in the public sector:

- Since integrity is a relevant factor of risk assessment and element of the internal control environment of the organisation, the effectiveness of the control systems in place is expected to increase.
- The establishment of the missing processes and/or relevant control activities is encouraged.
- The set up and functioning of ethical infrastructures in public bodies is stimulated and improved.
- Awareness of the importance of implementing and respecting ethical principles and values in public sector is increased.
- Relevant training and education on ethics is stimulated.
- A consistent application of the rules and regulations related to ethics and ethical behaviour is boosted.
- Ethical behaviour and ethical decision making are enhanced.
- Mechanisms for monitoring the implementation of ethical principles are strengthened.
- The number of breaches and irregularities may decrease.
- Fraud and corruption is prevented.

4.4 Ten golden rules of Integrity audit

Finally, to have a successful result of the audit, it is recommended to keep in mind these ten golden rules:

Scope: Integrity audits are for prevention, not for detecting fraud or corruption. The aim is to help improve integrity management by auditing the organisations risk control level.

Standards: For the framework it is important to include basic controls that are required by law or other regulations. Additional the framework can include other controls that are specific for the audited entity and that are needed to mitigate the auditees specific risks.

Benchmark: To ensure you have a lasting impact with your audit, see if you can use benchmarking techniques. For example publish the results of the audit of comparable organisations in one report and show relative weaknesses and strengths. This will stimulate completion and learning. Also try to repeat the audit after some time, so you can show progress or deterioration in the same entity. This will stimulate a lasting effect.

Introduction: For most auditees this approach will be new and strange. They will expect the SAI to try and detect integrity incidents, which they fear. Take care to explain the audit to the auditees. You are not looking for corruption but for what they can do to prevent corruption in a better way.

No surprises: Also good communication is important. Make sure you communicate the audit framework to the auditee and also make sure they understand it. And keep to it. Don't change it during the audit.

Involve and stimulate: One of the main advantages of this type of audit is that it gives the opportunity to raise awareness of integrity issues and risks within the public sector organisations. Also it shows the management what they can do to prevent integrity incidents in their organisation. And where possible try to also stress what is already going well. Compliments stimulate ownership.

Verify observations: After you gathered information and evidence, share you report of findings with the auditee and have the auditee check if the information in your report of findings is correct. This way you avoid the possibility for the auditee to oppose your final opinion by disputing the evidence.

Contradictory procedures: Usually the auditee will not be happy with your final report. To allow the auditees to give their own view on your report and publish this with your report, you make the result of the audit more palatable and you keep the communication line open for follow-up.

Publication: Of course transparency is important and the audit report should be open to the public, but you can choose how detailed your report is going to be. Try not to damage the reputation of the public sector, if that is not necessary. You can also think of different 'products' e.g. a paper report for the summary of a transversal audit and publication of more detailed information on your website. And you can also decide to share certain findings only with the auditee.

Follow-up: Don't just do one audit, but try to make it part of a theme or audit program. This will allow you to repeat audits to measure improvement. You can also consider to share your knowledge with other stakeholders, give lectures, training, write articles etc., etc.

Annex 1

Example Audit framework [14]

Integrity policy/codes of conduct
Has an integrity policy been formulated?
Is there a code of conduct?
Have measurable objectives been set for integrity policy?
Was management involved in formulating integrity policy?
Were the personnel involved in formulating integrity policy?
Has the policy been communicated to the personnel?
Are the policy and code of conduct based on risk analysis?
Are sanctions included in the policy or code of conduct?
Risk analysis
Have risks been analysed?
Was management involved in the risk analysis?
Were the personnel involved in the risk analysis?
Internal control of compliance with integrity policy
Are internal controls in place specifically for integrity policy?
Do the internal controls have an effect?
Audit
Does the auditor pay specific attention to compliance with integrity policy?
Do the audits lead to conclusions or recommendations?
Are lessons learned from the audit findings?
Is there a follow-up report?
Record of reports
Are reports of possible or actual unethical conduct recorded? *Is a record of violations or infringements present?*
Are there standard recording procedures?
Investigation of possible violations
Is every report of possible unethical conduct investigated?
Are there standard investigation procedures?
Are investigation reports available?
Are the scope, size and causes analysed?
Are lessons learned from the incidents?
Is there a follow-up report?

Reports to the Public Prosecution Service
Are suspected offences reported to the Public Prosecution Service?
Disciplinary action
Is a record kept of disciplinary action?
Policy evaluation
Is the policy or code of conduct evaluated?
Does the evaluation lead to conclusions or recommendations?
Is there a follow-up report?

[14] Netherlands Court of Audit *Integrity Management: A measurement of integrity management in 2004* http://www.courtofaudit.nl/english/Publications/Audits/Introductions/2005/04/Integrity_Management_a_base_line_measurement_in_2004

Criminal law/public office offences
forgery
breach of confidentiality
theft
extortion and blackmail
fraud
economic offences (insider trading, etc.)
abuse of authority or power
corruption and bribery (active or passive)
Central and Local Government Personnel Act, ARAR, ministerial orders, circulars
whistle-blowers' order
outside work/conflict of interests
regulations on the acceptance of gifts
revolving door arrangements
taking an oath of office
regulations on expense claims
information security (electronic or otherwise)
appointment of integrity advisers:
- integrity
- whistle-blowers
- sexual harassment and discrimination
Miscellaneous
vulnerable positions/screening
rules on the use of the internet and ministry property
rules on undesirable conduct
rules on the giving of gifts

Annex 2: IntoSAINT Integrity Control System

Cluster	Measure	
1		**Policy framework**
	1.1	Integrity measures embedded in a systematic policy framework
	1.2	Concrete objectives formulated as part of the integrity system
	1.3	Time and funds budgeted for implementing integrity measures
	1.4	Communication about Integrity measures
	1.5	Integrity policy formally laid down in an overall policy plan
2		**Vulnerability / risk analysis**
	2.1	General vulnerability / risk analyses regularly carried out
	2.2	In depth analyses carried out for vulnerable areas and positions
3		**Responsibilities**
	3.1	(Functional) responsibilities assigned for integrity
	3.2	Systematic consultation between officials responsible for integrity
	3.3	Integrity counsellor
	3.4	Periodic coordination with outside organisations and external stakeholders
	3.5	Coordinator appointed for integrity policy (externally)
4		**Integrity legislation and regulations**; Rules are in place regarding:
		Conflicts of interest
	4.1	- external positions/financial interests
	4.2	- the acceptance of gifts/invitations
	4.3	- confidentiality
	4.4	- preventing “revolving door arrangements”
	4.5	- external screening of contractors and/or licence applicants
	4.6	- lobbying
	4.7	- influence of politicians on civil servants
		Integrity within organisations
	4.8	- combating/dealing with undesirable conduct
	4.9	- expense claims
	4.10	- email, internet and telephone use
	4.11	- use of the employer’s property
5		**Administrative organisation and internal control**
	5.1	Specification of vulnerable activities and positions

Cluster	Measure	
	5.2	Specific procedures in place for conducting vulnerable activities
	5.3	Job descriptions for all staff members
	5.4	Segregation of duties
	5.5	“Four eyes principle” applied
	5.6	Mandate regulations
	5.7	Job rotation scheme
6		**Security**; Measures have been taken with regard to:
	6.1	physical security (locks, windows, doors, safes, etc.)
	6.2	Information security (IT security, clean desk policy, classification of information as confidential/secret, access authorisations, filing systems)
7		**Values and standards**
	7.1	Integrity is part of the organisation’s mission
	7.2	Core values have been formulated (e.g. impartiality, professionalism etc.)
	7.3	(Integrity) code of conduct
	7.4	Oath or pledge
	7.5	Special ceremony for taking the oath or pledge
8		**Integrity awareness**
	8.1	Integrity is an explicit requirement for all positions
	8.2	Regular training courses considering integrity
	8.3	Staff in vulnerable positions informed of particular risks and counter measures
	8.4	Special assistance and/or council for staff to cope with integrity risks
9		**Management attitude**
	9.1	Management actively promotes the importance of integrity
	9.2	Management actively seeks the implementation of an integrity policy and integrity measures
	9.3	Management always responds appropriately to integrity issues
	9.4	Management itself complies with integrity regulations and/or code of conduct
10		**Organisational culture**
	10.1	Regular attention is paid to the importance of integrity
	10.2	Integrity questions can be discussed safely
	10.3	Sufficient opportunity to express criticism
	10.4	Importance of integrity is clearly explained to external relations
	10.5	Open communication on integrity violations and how they are dealt with
	10.6	Culture of holding others responsible for their conduct
	10.7	Sufficient consideration of job satisfaction

Cluster	Measure	
11		**Recruitment & selection**
	11.1	Fixed procedures for dealing with all applications
	11.2	Advisory selection committee
	11.3	Checking of CVs, diplomas, references, etc.
	11.4	Pre-employment screening on qualifications and moral integrity
	11.5	Integrity is part of the introduction programme for new members of staff
	11.6	Declaration of confidentiality signed by staff
	11.7	Integrity is periodically considered in work consultation meetings and performance interviews
	11.8	Integrity is a specific consideration when hiring temporary and external staff
	11.9	Integrity is considered when staff leave or during exit interviews
12		**Response to integrity violations**
	12.1	Notification procedure in place for employees to report suspected violations ('whistle blowers procedure')
	12.2	Managers are accessible by employees to report suspected violations
	12.3	Integrity counsellor is involved in the notification of violations
	12.4	Procedure for handling signals and complaints from external sources
	12.5	Protocol for investigating (suspected) integrity violations
	12.6	Central recording of integrity violations
	12.7	The organisation always responds to integrity violations
	12.8	Suspicions of criminal offences are always reported to the public prosecutor or the police
	12.9	Incidents are evaluated and discussed with staff involved
13		**Accountability**
	13.1	Senior management receives reports to account for the integrity policy conducted
	13.2	Staff representatives receive reports to account for the integrity policy conducted
	13.3	Democratically elected authorities (parliament, municipal council, etc.) receive reports to account for the integrity policy conducted
	13.4	Reports are systematically structured and containing clear indicators
14		**Audit & monitoring**
	14.1	The integrity system is periodically audited by an internal auditor
	14.2	The integrity system is periodically reviewed by an external auditor and/or supervisor
	14.3	The integrity system is periodically monitored or evaluated by management