Court of Accounts Republic of Moldova

INTEGRITY SELF ASSESSMENT
14-07-2016

Assessment report

Moderators: Viorica Verdeş, Irina Gutnic, Iulian Dumitraş (Court of Accounts Moldova),
Noëlle Ruckert (Netherlands Court of Audit)
Contact person SAI: Viorica Verdeş

Contents

Introduction

This report reflects the results of the integrity self assessment of the Supreme Audit Institution of Moldova. The self assessment was conducted applying the SAINT methodology as provided by the Netherlands Court of Audit (NCA) for members of Intosai (IntoSAINT).

The focus of the self assessment was the whole organisation.

The basic concepts of integrity and the SAINT methodology may be summarised as follows:

- Integrity implies not only observing rules and laws but also a moral responsibility.
- Integrity is a quality aspect of an organisation and therefore a responsibility of management.
- Integrity is an essential condition for trust in the public sector.
- Prevention and awareness of existing vulnerabilities is most effective to protect the integrity of an organisation.
- Organisations may prevent integrity breaches by reducing their vulnerability and by having a mature integrity control system in place.
- A mature integrity system consists of general, hard and soft controls.
- Employees as insiders are usually in a good position to identify vulnerabilities, to detect weaknesses in the integrity control system and to identify ways to improve the resilience to integrity breaches.
- Participation of employees in the assessment of integrity raises the awareness about the issue of integrity .

.

The self assessment was performed on the 12th and 13th of July 2016 by a carefully selected group of employees from strategic positions in the organisation. A list of participants is included in Annex 1. During the workshop the participants went through the various steps of the self assessment methodology.

This management report first provides a summary of the outcome of the self-assessment and then continues to describe the results of the consecutive steps of the method:

a. description of the selected organisational processes;
b. identification of the vulnerability profile;
c. the maturity of the existing integrity control system;
d. the analysis of the gap between the vulnerability profile and the integrity control measures the organisation has in place.

On the basis of these descriptions, recommendations are formulated to reduce the vulnerability and to improve the integrity control system.

We would like to acknowledge the co-operation we received from the Court of Accounts of the Republic of Moldova to conduct the SAINT workshop, especially the efforts of the workshop participants, the workshop coordinator, the co-moderators and the support of the staff.

Summary

PM

1 Description of organisational processes

Before the start of the workshop a pre-selection of key-processes of the Court of Accounts of the Republic of Moldova was prepared in cooperation between the contact person and moderators from the Court of Accounts of the Republic of Moldova. During the workshop this and selection was discussed and the participants confirmed to focus the self assessment on the following processes.

The vital organisational processes involved are :

Primary processes:
- Monitoring the audit environment
- Audit processes
- Development processes. Allocate lot of resources to this.
- International activities / protocol.
- Making audit results public (transparency)

Secondary processes:
- Personnel / HRM
- Professional development: training
- Financial management: claiming budget, monitoring use of budget.
- Information management (including information security)
- Facility management (including physical security)
- Archiving

Management and control processes:
- Strategic planning
- Monitoring of the implementation of policies (of the Court of Accounts of Moldova)

This list of processes served as reference for the other steps of the IntoSAINT workshop.

2 Vulnerabilities

2.1 Inherent vulnerabilities

All organisations are to some extent vulnerable for integrity breaches. However certain activities and functions in the public sector are specifically vulnerable. These are called inherent vulnerabilities and are usually related to the specific tasks of an organisation. During the workshop the processes and functions of the Court of Accounts of the Republic of Moldova have been compared with a list of inherent vulnerabilities, as indicated in the table below.

	Vulnerable areas /activities /actions		**Average score[1]**	**Level**
Relationship of the entity with its environment	Contracting	procurement, tenders, orders, assignments, awards	1.82	High
	Payment	subsidies, benefits, allowances, grants, sponsoring	0.71	Low
	Granting / Issuance	permits, licenses, identity cards, authorizations, certificates	0.18	Low
	Regulating	conditions of permits, setting standards / criteria	0.18	Low
	Inspection / audit	supervision, oversight, control, inspection, audit	2.59	High
	Enforcement	prosecution, justice, sanctioning, punishment	1.71	High
Managing public property	Information	national security, confidential information, documents, dossiers, copyright	2.35	High
	Money	treasury, financial instruments, portfolio management, cash/bank, premiums, expenses, bonuses, allowances, etc.	1.82	High
	Goods	handling, management and consumption (stocks, computers)	1.47	Medium
	Real estate	buying / selling	0.44	Low

In the two columns on the right, the table indicates the average scores of the workshop participants and the level of inherent vulnerability.

This level may be low, medium or high, based on the following criteria:

Average score	**Level**
average < 0,8	Low
0,8 ≤ average ≤ 1,6	Medium

[1] Legenda: 0 = not important, 1 = relevant, 2 = important, 3 = very important

average > 1,6	High

The average inherent vulnerability identified during the workshop is on a medium level. From the table can be concluded that the most relevant vulnerable areas are (in order of relevance):

- Inspection / audit
- Information
- Contracting
- Money
- Enforcement

Further discussion revealed that the score for 'money' might be a little high, as the employees of the Court of Accounts of Moldova don't have very many processes involving money. Money mostly involves wages.
Also, with regard to enforcement, it should be noted that the Court of Accounts of Moldova does not have a direct authority. Its findings can be evidence in a court however and be used in rulings to impose fines.

2.2 Vulnerability enhancing factors

In addition to the inherently vulnerable activities, some circumstances or factors may enhance the vulnerability to integrity violations. These factors can increase vulnerability because:

- they increase the probability of an incident occurring;
- they increase the consequences (impact) of an incident (not only financially but also with regard to credibility, working atmosphere, relations, image, etc.).

Many of the Vulnerability enhancing circumstances or factors provide opportunity and/or motivation and/or rationalisation for breaches of integrity. Other factors are known as indicators of a (potentially) weak integrity culture within an organisation.
It must be stressed that presence of one or more of these factors does not imply that breaches of integrity are taking place. It merely implies that the organisation is more vulnerable and that there is a higher risk of integrity breaches.

During the workshop the workshop participants evaluated and discussed the full list of vulnerability enhancing factors. This list and the average score per vulnerability enhancing factor can be found in Annex 2.

The average scores of the workshop participants per cluster and the resulting level of vulnerability are indicated in the table below.

Clusters of vulnerability enhancing factors	**Average score (0-3)[2]**	**Level**

[2] Legenda: Legenda: 0 = not important, 1 = relevant, 2 = important, 3 = very important

1. Complexity	0.94	Medium
2. Change/Dynamics	0.9	Medium
3. Management	1.05	Medium
4. Personnel	0.9	Medium
5. Problem history	0.41	Low
Overall average score	0.89	Medium

Similar to the inherent vulnerabilities, the level of enhanced vulnerability may be low, medium or high, based on the following criteria:

Average score	**Level**
average < 0,8	Low
0,8 ≤ average ≤ 1,6	Medium
average > 1,6	High

We can specify the assessment of the vulnerability enhancing factors per cluster, which makes it possible to identify underlying reasons for the level of the cluster scores (see annex 2).

From the table can be concluded that the most relevant vulnerability enhancing factors are:
- Management
- Complexity
- Change/dynamics
- Personnel

However, it should be noted that all these scores are in the low range of the medium category.

One of the main concerns of the participants had to do with the way parliament perceives the role of the Court of Accounts. One of the (implied) criticisms seems to be that the Court of Accounts does not make sure that recommendations are followed-up. Making the Court of Accounts an organization with limited effectiveness (it 'barks but does not bite'). Since the root of the problem of this misperception lies in the information position of Parliament, this can only be remedied by communication. One of the participants noted that there is a positive development. The added value of an organization that signals problems within the government is increasingly seen.
Another concern that was voiced was that in the coming period, the workload is expected to get heavier, due to some legislative changes which increase the number of organizations that need to be audited by the CCA. No provisions have been made to increase the audit capacity however. Ultimately, this may construe a risk to the quality of the audit work.

Summarized, the following additional remarks were made when we discussed the most relevant vulnerability enhancing factors, as listed above:

- Management does not pay enough attention to the opinion / advice of the auditors when planning / choosing / defining audits
- A different interpretation of legal provisions is possible. Also, the same norm is included in different normative acts (tax and customs acts) leaving room for interpretation. Ultimately, this means that certain audit findings have to be decided on in a court of law, instead of by the Court of Accounts itself.
- The members of the Court of Accounts are appointed by parliament for a five year period. This gives parliament political influence, even though members, once appointed are required to be politically neutral.
- Parliament is selective in its attention to the findings of the Court of Accounts: it pays more attention to those findings which are favourable to their political faction. Also, some audit results do not get any attention from parliament at all.
- There is a high level of employee turnover[3]. This leads to a loss of knowledge and loss of capacity due to the necessity of helping new colleagues get settled in. This can be a risk to the audit quality. An important cause of this high turnover is felt to be the (low) wage level, as this is often cited as a reason to leave. On the other hand, this could also be a 'natural' thing: people are always looking for ways to improve their position.
- An employee can get a variable wage of up to 15% added to his or her base salary over 6 months dependent on performance. The quality of performance is determined by the immediate superior.

The Court of Accounts submitted to the Parliament a project of a new law which intends to reorganise the structure of the institution. With the approval of the new law some of the vulnerabilities will be diminished. The new law contains provisions on the remuneration policy as well it will solve the issues related to the political influence. In this regard, the general auditor will be appointed on the period of 7 years instead of 5 years, as well as the board of members will be replaced by the general auditor and 2 vice-general auditors.

2.3 Vulnerability profile

The overall level of vulnerability, the vulnerability profile is based on the overall 'picture' of the inherent vulnerabilities and the vulnerability enhancing factors. The combined levels of inherent vulnerabilities and vulnerability enhancing factors lead to the overall level of vulnerability.

The level of inherent vulnerability as assessed by the workshop participants is medium. The level of enhanced vulnerability is medium. Together this results in a medium vulnerability profile. This vulnerability profile is taken into account when comparing this level with the maturity level of the integrity control system and plays a role as part of the gap analysis.

[3] The actual percentage of turnover is 9% annually. According to international standards, this is a medium turnover

3 Maturity level Integrity Control System

A key element of the 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.

The organisation's integrity control system is described using an extensive set of integrity measures divided into three main groups (general, hard and soft controls).

The hard controls, as the term suggests, are concerned chiefly with regulations, procedures and technical systems. The soft controls are designed to influence behaviour, working atmosphere and culture within the organisation. The clusters in the general controls category are more wide ranging or have a mix of hard and soft elements.

The outcome of the assessment of the integrity control system is shown below per cluster of measures.

Nr.	Clusters of controls	Average	Level
	General controls		
1	Policy framework	2.26	High
2	Vulnerability / risk analysis	1.82	Medium
13	Recruitment and selection	2.63	High
14	Response to integrity violations	2.64	High
15	Accountability	2.53	High
16	Audit and monitoring	1.98	Medium
	Hard controls		
3	Responsibilities	2.24	High
4	SAI legal framework	2.76	High
5	Integrity legislation and regulations	2.24	High
6	Administrative organisation and internal control	2.39	High
7	Security	2.97	High
	Soft controls		
8	Values and standards	2.95	High
9	Professional SAI standards	2.68	High
10	Integrity awareness	2.29	High
11	Management attitude	2.57	High
12	Organisational culture	2.37	High
	Overall average score of all clusters	**2.46**	**High**

The assessment of the maturity level of the integrity control system takes into account the existence, the implementation, the operation and the performance of controls. The scores on the individual measures range from 0, when a measure is non existent, to 3 when a measure exists, is observed and effective, as indicated in the following table.

Level	Criteria
0 – Low	▪ The measure does not exist
1 – Low	▪ The measure exists ▪ The measure is not implemented / not observed
2 – Medium	▪ The measure exists ▪ The measure is implemented / observed ▪ The measure is not effective
3 - High	▪ The measure exists ▪ The measure is implemented / observed ▪ The measure is effective

In principle, the highest level, maturity level 3, is required. Scores for individual measures lead to cluster scores and in the end to an overall level of maturity for the integrity control system as a whole. The comprehensive integrity control system and the maturity scores per control measure can be found in Annex 3.
The overall average score determines the level of maturity of the integrity control system as a whole. See the table below.

Score maturity of the Integrity Control system	Level	
$0 \leq x \leq 1$	1	Low
$1 < x \leq 2$	2	Medium
$2 < x \leq 3$	3	High

The table shows that the overall maturity level of the body of measures is high. The main strengths of the system can be found in security and values and standards. The main weaknesses are in Vulnerability / risk analysis and audit / monitoring. However, the maturity level of these controls are still assessed as medium.

Generally, it can be said that that soft controls have a very high level of maturity. They scored higher than the hard, and especially the general controls. It was felt that, because of the high level of maturity of the soft controls, general controls did not need to score as high. Within the category of soft controls, what scored highest was ‘values and standards’. Integrity policy is a part of the organizational environment. In this regard, the Court of Accounts has developed and approved a code of conduct which contains a set of rules and behavioural standards for auditors. These are derived from international standards and the national legislative framework. Special attention is given to the implementation of this code of conduct. Newcomers are familiarized with the provisions of this policy. Additionally, for the new civil servants, the oath or pledge is mandatory. There is a special ceremony for this.

The following remarks were made with regard to the controls:

General controls

- Elements of the integrity policy are embedded in: national normative acts, the law of the Court of Accounts, the institutional development strategy, code of conduct, quality guidelines, internal regulations and regulations on gifts and declarations.

- Communication about integrity measures is being done in several ways:: internal training, sending the information through e-mail and on the internet page of the Court of Accounts.
- The Court of Accounts ensures that the information was received / people are aware of what was discussed by: lists of attendance (for trainings), confirmation that e-mail was received
- Recruitment and selection: procedure is adhered to strictly. Personnel is recruited following a legal procedure and has been made as objective as possible. There are 2 rounds: a written one, leading to a first selection and after that an interview. Questions for the interview are standardized. The decision is taken by a committee which consist of 5 people from different levels of responsibility within the Court of Accounts.
- Reaction to integrity breaches of integrity: integrity violations in the past have been acted upon. There is a disciplinary committee which is entitled to examine cases of suspected integrity violations and can present their findings to the president. The president ultimately takes a decision on disciplinary measures. The exact procedure was not known to everyone, but the result (the disciplinary measures imposed) was visible.
- Integrity responsibility: there is a normative framework on integrity and there is systematic reporting. Not everyone knows about this however.
- Audit and follow up: external audit on the financial report is not done. But an external assessment on integrity is done by NGO's (Transparency International). In this report the Court of Accounts was ranked as one of the least corrupt organizations.

Hard controls

- Security: the Court of Accounts has both a high level of IT security and physical security. Every auditor has his own pc, with his own password and a closed internet network. There is a mandatory monthly change of passwords. Physical security of Court of Accounts property and goods is ensured by checks on entrance access.
- The Court of Accounts reports periodically to the national agencies regarding the level of implementation of nationals policies on integrity and prevention of corruption. The monitoring and the reports are drafted / presented by a small team from the institution. Participants were not aware of this. This is why there was a low score on the measure on 'integrity co-ordinator'.

Soft controls:

- A lot of trainings are organized for personnel on integrity (included in training plans but not as the sole topic)
- There is someone who is responsible for dealing with fraud and corruption, but he / she is not responsible for the other aspects of integrity (preventative). It is necessary to intensify to broaden the range of activities of an integrity counsellor / co-ordinator.
- Personnel restrictions to appoint an integrity counsellor (there is no provision for this in normative / legal acts)

The detailed scores on the maturity levels were used by the workshop participants to discuss potential improvements in the integrity control system. The participants also considered what controls were already on a satisfactory level or did not need improvement, because they do not apply tot the situation within the Court of Accounts of Moldova or would cause too much

bureaucracy, relative to their contribution to the integrity control system. The ultimate results from this exercise are reflected in the chapter on recommendations.

4 Gap analysis and recommendations

4.1 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. Even in case of a balance between the level of vulnerability and the maturity level of the integrity controls, it may still be desirable to reduce some of the identified vulnerabilities or to address specific controls that need strengthening.

During the workshop the participants conducted an assessment on the general level of vulnerabilities and resilience. For the Court of Accounts of the Republic of Moldova the workshop established an (im)balance between the vulnerability profile (level: medium and the maturity level of the integrity control system (maturity level: high).
The maturity level of the integrity control system thus exceeds the level of vulnerability. However, participants did not feel that this result warranted 'scaling down' the integrity control system. Since, in their view, it was still possible to reduce some vulnerabilities and certain areas of the Integrity Control system could still be strengthened, recommendations to this were discussed.

4.2 Recommendations

Based on the assessment of the vulnerabilities and the (maturity level of) the integrity control system the workshop participants formulated a number of recommendations to management. These recommendations may be clustered by theme as follows.

Recommendations aimed at reducing vulnerabilities

- Increase the wages
- Involvement of the auditors in the audit planning process
- Ensure that the same auditors carry out the follow -up assignments
- Avoid consecutive appointment of the same auditors for audit missions that have as subjects same auditees
- Monitoring of changes in the regulatory framework
- Improve the communication with the Parliament, as a result of approving the regulation regarding the cooperation with Parliament, in order to enhance the level of implementation of audit recommendations.

Recommendations developed in order to strengthen internal control system of integrity:

- Organise trainings on integrity topics
- Carry out the personality test of CoA employees (MBTI)
- Update the risk register (in terms of integrity risks) and actions developed to mitigate those risks
- Improve the internal communication

We believe the implementation of the recommendations presented in this chapter will contribute to improving the integrity awareness and the integrity control system within the Court of Accounts of Moldova.

Annex 1 List of participants

Chiosa Aurel	controlor de stat principal
Certan Alina	controlor de stat principal
Andrieș Violeta	controlor de stat principal
Bulmaga Liuba	controlor de stat superior
Secrieru Vasile	controlor de stat
Baxanean Natalia	controlor de stat superior
Caraman Tatiana	controlor de stat
Babanuța Irina	controlor de stat
Zamăneagră Lilia	controlor de stat superior
Ceban Larisa	controlor de stat
Pavalachii Iulian	controlor de stat
Bogatîreț Reghina	controlor de stat principal
Stegărescu Ludmila	consultant superior
Balan Violeta	șef Serviciu
Triboi Tatiana	specialist principal
Oprea Tatiana	specialist principal
Ciolan Alina	redactor principal

Contact person:

Viorica Verdeş

Annex 2 Vulnerability enhancing factors

	Score (0-3)
1. Complexity	
1.1 Innovation / advanced computer) systems	0,94
1.2 Complex legislation	1,47
1.3 Special constructions (legal / fiscal)	0,47
1.4 Bureaucracy	1,35
1.5 Lobbying	0,65
1.6 Networks of relations	1,12
1.7 Mix of public-private interests (commerce / competition)	0,47
1.8 Need for external expertise	0,59
1.9 Political influence / intervention	1,41
2. Change/Dynamics	
2.1 Young organisation	0,35
2.2 Frequently changing legislation	1,24
2.3 Strong growth or downsizing	1,24
2.4 Privatisation / Management buy-out	0,29
2.5 Outsourcing	0,71
2.6 Crisis (reorganisation, threats with huge impact, survival of the organisation or job at stake)	1,18
2.7 External pressure (pressure on performance, expenditure, time, political pressure, shortages / scarce resources in comparison with duties)	1,29
3. Management	
3.1 Dominant	1,12
3.2 Manipulative	0,82
3.3 Formal / bureaucratic	1,00
3.4 Solistic operation	0,88
3.5 Remuneration strongly dependent on performance	1,12
3.6 Lack of accountability	0,94
3.7 Ignoring advice / signals	1,29
3.8 Defensive response to criticism or complaints	1,24
4. Personnel	
Work environment / Loyalty	
4.1 Pressure on performance / income dependent on performance	1,24
4.2 Low status / lack of esteem/ low rewards/ low career prospects	1,35
4.3 Poor working conditions/ High workload	1,00
4.4 Group loyalty	1,00
4.5 Power to obstruct	1,00
Individual	

4.6 Having other interests (side jobs etc.)	0,47
4.7 Personal debts	0,82
4.8 Lifestyle (overspending)	1,06
4.9 Personal secrets (vulnerable for blackmail)	0,94
4.10 Personal threats	0,65
4.11 Addictions (alcohol, drugs)	0,35
5. Problem history	
5.1 Complaints	0,53
5.2 Gossip and rumours	0,88
5.3 Signals / whistle blowers	0,94
5.4 Earlier incidents (recidivism)	0,53
5.5 Administrative problems (backlogs, inconsistencies, extraordinary trends etc.)	0,41

Annex 3 Integrity control system

Cluster	Measure		Maturity level
1		**Policy framework**	
	1.1	Integrity measures embedded in a systematic policy framework	2,59
	1.2	Concrete objectives formulated as part of the integrity system	2,35
	1.3	Time and funds budgeted for implementing integrity measures	1,82
	1.4	Communication about Integrity measures	2,35
	1.5	Integrity policy formally laid down in an overall policy plan	2,18
		Average cluster score	**2,26**
2		**Vulnerability / risk analysis**	
	2.1	General vulnerability / risk analyses regularly carried out	1,88
	2.2	In depth analyses carried out for vulnerable areas and positions	1,76
		Average cluster score	**1,82**
3		**Responsibilities**	
	3.1	(Functional) responsibilities assigned for integrity	2,53
	3.2	Systematic consultation between officials responsible for integrity	2,06
	3.3	Integrity counsellor	2,41
	3.4	Periodic coordination with outside organisations and external stakeholders	2,18
	3.5	Coordinator appointed for integrity policy (externally)	2,00
		Average cluster score	**2,24**
4		**SAI legal framework**	
	4.1	Existence and independence of the SAI embedded in the Constitution (ISSAI 10; principle 1)	2,94
		A legal framework is in place to guarantee:	
	4.2	- the independence of SAI heads and members (of collegial institutions), including security of tenure and legal immunity in the normal discharge of their duties (ISSAI 10, principle 2)	2,76
	4.3	- a sufficiently broad mandate and full discretion, in the discharge of SAI functions (ISSAI 10, principle 3)	2,65
	4.4	- unrestricted access to information (ISSAI 10, principle 4)	2,71
	4.5	- the right and obligation to report on the SAIs work and the freedom to decide the content and timing of audit reports and to publish and disseminate them (ISSAI 10, Principle 5/6)	3,00
	4.6	- financial and managerial / administrative autonomy and the availability of appropriate human, material and monetary resources (ISSAI 10, principle 8)	2,53
		Average cluster score	**2,76**
5		**Integrity legislation and regulations**; Rules are in place regarding:	
		Conflicts of interest	
	5.1	- external positions/financial interests	2,47
	5.2	- the acceptance of gifts/invitations	2,76

Cluster	Measure		Maturity level
	5.3	- confidentiality	2,82
	5.4	- preventing “revolving door arrangements”	2,12
	5.5	- external screening of contractors and/or licence applicants	1,29
	5.6	- lobbying	1,59
	5.7	- influence of politicians on civil servants	2,00
		Integrity within organisations	
	5.8	- combating/dealing with undesirable conduct	2,24
	5.9	- expense claims	2,65
	5.10	- email, internet and telephone use	2,06
	5.11	- use of the employer’s property	2,65
		Average cluster score	**2,24**
6		**Administrative organisation and internal control**	
	6.1	Specification of vulnerable activities and positions	2,18
	6.2	Specific procedures in place for conducting vulnerable activities	1,82
	6.3	Job descriptions for all staff members	3,00
	6.4	Segregation of duties	3,00
	6.5	“Four eyes principle” applied	2,88
	6.6	Mandate regulations	2,88
	6.7	Job rotation scheme (ISSAI 40, 6b, element 2)	1,00
		Average cluster score	**2,39**
7		**Security**; Measures been taken regarding:	
	7.1	physical security (locks, windows, doors, safes, etc.)	3,00
	7.2	Information security (IT security, clean desk policy, classification of information as confidential/secret, access authorisations, filing systems)	2,94
		Average cluster score	**2,97**
8		**Values and standards**	
	8.1	Integrity is part of the organisation’s mission	3,00
	8.2	Core values have been formulated (e.g. impartiality, professionalism etc.)	2,94
	8.3	(Integrity) code of conduct	3,00
	8.4	Oath or pledge	3,00
	8.5	Special ceremony for taking the oath or pledge	2,82
		Average cluster score	**2,95**
9		**Professional SAI standards**	
	9.1	The SAI is not involved (or seen to be involved) in any matter whatsoever, in the management of the organizations that it audits (ISSAI 11, principle 3, Guidelines)	2,76
	9.2	In working with the executive, auditors do act only as observers and do not participate in the decision-making process (ISSAI 11, principle 3, Guidelines)	2,65
	9.3	Guidelines issued by the SAI to ensure that its personnel does not develop too close a relationship with the entities they audit, so that they remain objective and appear objective (ISSAI 11, principle 3, Guidelines)	2,76

Cluster	Measure		Maturity level
	9.4	Training courses offered to staff introducing the importance of independence into the SAIs culture and emphasizing the required quality and performance standards, ensuring that work is autonomous, objective and without bias (ISSAI 11, principle 3, Good Practices)	2,65
	9.5	The SAI has a code of (professional) ethics and standards with ethical significance in place, covering: - trust, confidence and credibility (ISSAI 30, chapter 1); - integrity (ISSAI 30, chapter 2); - independence, objectivity, impartiality, (political) neutrality, avoidance of conflicts of interests (ISSAI 30, chapter 3; ISSAI 200/2.1-2.32); - professional secrecy (ISSAI 30, chapter 4); - due care and competence (ISSAI 30, chapter 5; ISSAI 200/2.1, 2.33-2.46).	3,00
	9.6	Employees have been involved in the formulation of the code of ethics and/or the standards with ethical significance	2,24
		Average cluster score	**2,68**
10		**Integrity awareness**	
	10.1	Integrity is an explicit requirement for all positions	2,88
	10.2	Regular training courses considering integrity	1,65
	10.3	Staff in vulnerable positions informed of particular risks and counter measures	2,29
	10.4	Special assistance and/or council for staff to cope with integrity risks	2,35
		Average cluster score	**2,29**
11		**Management attitude**	
	11.1	Management actively promotes the importance of integrity	2,71
	11.2	Management actively seeks the implementation of an integrity policy and integrity measures	2,41
	11.3	Management always responds appropriately to integrity issues	2,59
	11.4	Management itself complies with integrity regulations and/or code of conduct, serving as an example of appropriate ethical behaviour (ISSAI 40, 6b, element 2)	2,59
		Average cluster score	**2,57**
12		**Organisational culture**	
	12.1	Regular attention is paid to the importance of integrity	2,65
	12.2	Integrity questions can be discussed safely	2,65
	12.3	Sufficient opportunity to express criticism	2,00
	12.4	Importance of integrity is clearly explained to external relations	2,59
	12.5	Open communication on integrity violations and how they are dealt with	2,18
	12.6	Culture of holding others responsible for their conduct	2,65
	12.7	Sufficient consideration of job satisfaction	1,88
		Average cluster score	**2,37**
13		**Recruitment & selection**	
	13.1	Fixed procedures for dealing with all applications	2,94
	12.2	Advisory selection committee	2,82

Cluster	Measure		Maturity level
	13.3	Checking of CVs, diplomas, references, etc.	2,76
	13.4	The members and the audit staff of the SAI are evaluated (pre-employment screening) on their qualification and moral integrity required to completely carry out their tasks (ISSAI 1: Lima declaration; Section 14.1)	2,65
	13.5	Integrity is part of the introduction programme for new members of staff	2,76
	13.6	Declaration of confidentiality signed by staff	2,65
	13.7	Integrity is periodically considered in work consultation meetings and performance interviews	2,47
	13.8	Integrity is a specific consideration when hiring temporary and external staff (ISSAI 40, 6b, element 2)	2,47
	13.9	Integrity is considered when staff leave or during exit interviews	2,12
		Average cluster score	**2,63**
14		**Response to integrity violations**	
	14.1	Notification procedure in place for employees to report suspected violations ('whistle blowers procedure') (ISSAI 40, 6b, element 2)	2,41
	14.2	Managers are accessible by employees to report suspected violations	2,76
	14.3	Integrity counsellor is involved in the notification of violations	2,65
	14.4	Procedure for handling signals and complaints from external sources	2,76
	14.5	Protocol for investigating (suspected) integrity violations	2,65
	14.6	Central recording of integrity violations	2,71
	14.7	The organisation always responds to integrity violations	2,82
	14.8	Suspicions of criminal offences are always reported to the public prosecutor or the police	2,12
	14.9	Incidents are evaluated and discussed with staff involved	2,88
		Average cluster score	**2,64**
15		**Accountability**	
		General	
	15.1	Senior management receives reports to account for the integrity policy conducted	2,59
	15.2	Staff representatives receive reports to account for the integrity policy conducted	2,29
	15.3	Democratically elected authorities (parliament, municipal council, etc.) receive reports to account for the integrity policy conducted	1,88
	15.4	Reports are systematically structured and containing clear indicators	2,00
		SAI specific	
	15.5	The SAI's mandate, role, responsibilities, organization, mission, strategies, audit manuals, procedures and criteria are public (ISSAI 20, chapter 2/3)	3,00
	15.6	The SAI's audit findings and conclusions are subject to contradictory procedures (consultation with the audited entity) (ISSAI 20, chapter 3)	3,00
	15.7	The SAIs accounts are public and subject to external audit or parliamentary review (ISSAI 20, chapter 4)	1,59
	15.8	The SAI is open about measures to prevent corruption and ensure clarity and legality in its own operations (e.g. disciplinary sanctions) (ISSAI 20, chapter 5)	2,76
	15.9	The status of auditors (magistrates in the Court model, civil servants or others), their powers and obligations are public (ISSAI 20, chapter 5)	2,76

Cluster	Measure		Maturity level
	15.10	Outsourcing, expertise and sharing audit activities with external entities, public or private, are performed under the responsibility of the SAI and subject to precise rules (ISSAI 20, chapter 5)	2,47
	15.11	Codes of ethics are issued and public (ISSAI 20, chapter 5)	3,00
	15.12	The SAI issues public reports on audit findings, management, performance and communicate openly with the media or other interested parties (ISSAI 20, chapter 6)	3,00
		Average cluster score	**2,53**
16		**Audit & monitoring**	
	16.1	The integrity system is periodically audited by an internal auditor	1,41
	16.2	The integrity system is periodically reviewed by an external auditor and/or supervisor	1,76
	16.3	The integrity system is periodically monitored or evaluated by management	2,76
		Average cluster score	**1,98**
		Total score = average score of all clusters	**2,46**

Annex 4: complete list of recommendations

Implementation horizon

Recommendation	short term	medium term	long term
Increase the wages	13		
Involvement of the auditors in the audit planning process	4	7	1
Carry out the personality test of CoA employees (MBTI)	2	3	6
Ensure that the same auditors are carrying out the follow -up assignments	4	2	3
Update the risk register (in terms of integrity risks) and actions developed to mitigate those risks			9
Avoiding consecutively appointment of the same auditors for audit missions that has as subjects same auditees	7	2	
Monitoring of changes in the regulatory framework		2	7
Improve the internal communication	5	4	
Improve the communication with the Parliament, as a result of approving the regulation regarding the cooperation with Parliament, in order to enhance the level of implementation of audit recommendations.		3	4
Organise trainings on integrity topics		6	
Adjust the methodological framework regarding the selection of audit topics with the proper justification of choosing it		4	2
Implementation of the provisions of Communication Strategy and of Code Ethics and of coaching managerial procedures	1	4	1
Revise and adjust the members of staff according to the new mandate		3	2
Ensure the continuity of training related to the writing of recommendations	1	2	2
Continue the process of identification of law deficiencies			3
Disseminate the information related to the possibility of employees to be consulted on integrity aspects		2	