OFFICE OF THE AUDITOR GENERAL OF BELIZE

INTEGRITY SELF-ASSESSMENT

September 2nd, 3rd and 4th, 2015

Assessment Report

Final version

Moderators of the *Supreme Audit Institution of Mexico*

- **Miss Paola Carvajal-González,** Administrative Auditor "A" at the Research and National Auditing System Department, and IntoSAINT moderator.
- **Mr. Francisco T. Parral-Pineda,** Supervisor at the International Relations Department, and IntoSAINT moderator.

Liaison officers at the *Office of the Auditor General of Belize*

- **Mrs. María Rodríguez,** Supervisor of Audit and liaison officer to OLACEFS.
- **Mr. Edmund Zuniga,** Examiner of Accounts and IntoSAINT moderator.

This report is confidential.
The information in this report is exclusively intended for use by SAI of Belize.

Contents

Executive summary

An Integrity Self-Assessment Workshop (IntoSAINT*)* aims to allow Supreme Audit Institutions (SAI) to evaluate their institutional vulnerability and the strength of their Integrity Control Systems (ICS) against possible violations to integrity, having a composite product: this Report to the SAI of Belize's Top Management as well as training and awareness to the workshop participants on integrity issues. The knowledge value gained by the 15 participants of the Office of the Auditor General of Belize is essential, and they are expected to contribute as agents of change and advocates of the strengthening and awareness of integrity in the institution.

The Integrity Self-Assessment Workshop was developed in strict accordance with the IntoSAINT methodology. The results of the workshop showed that there are internal opportunity areas in different cases related to integrity matters (awareness, organizational climate, training, professional development, etc.). It is essential that the measures implemented are properly articulated, operated and widely disseminated. Therefore, it is advisable to advance these efforts, in order to promote new mechanisms and strengthen existing ones.

During the workshop, it was identified that the SAI of Belize does have technical autonomy for the discharge of its duties. However, the dependence on the Ministry of Public Service could affect the institutional autonomy in financial and management terms. This must be understood as a structural situation related to the public sector in Belize in general, and that legislative change requires time.

To do this, the participants, guided by the moderator team, have identified opportunity areas and created, in consequence, recommendations to be considered by the Top Management, as to promote internal control measures and to ensure sustainability in the long term by including integrity in the institutional policy framework.

A prioritization or a chronological implementation of recommendations are not proposed because this situation goes beyond the scope of the IntoSAINT methodology, and is considered as a decision that must be taken by the Top Management.

Opportunity areas that have been identified are classified in eight different clusters:

1 **Integrity Policy Framework.** It is truly convenient to adopt a comprehensive integrity policy framework, which includes different elements and specific activities to promote the integrity management, including its monitoring, evaluation and dissemination.

2 **Internal Control Framework.** By having an Internal Control Framework the institution will strengthen its strategy to achieve institutional objectives in all areas and levels within the organization. This includes mechanisms such as the implementation of risk analysis and the safeguard of information.

3 **Prevention.** This cluster aims to prevent integrity violations by foreseeing potential risks. Strategies such as installed-capacity and required-equipment diagnosis, as well as civil protection measures, are considered.

4 **Organizational environment.** These measures aim to foster job satisfaction and public servants' better performance in the institution.

5 **Capacity-building and training.** To encourage personnel' skills and professional development in order to be better prepared for the discharge of their duties.

6 **Leadership.** Top Management's leadership in integrity matters is convenient, since their actions have an impact in the whole institution. Top Management's attitude will inspire the staff to behave in a professional way.

7 **Communication strategy.** This strategy aims to strengthen cross-sectional communication, including a top-down and bottom-up approach.

8 **Promotion of good governance.** A great opportunity has been found for the SAI of Belize to promote integrity and good governance in the public sector in the country.

Introduction

This report reflects the results of the Integrity Self-Assessment of the Supreme Audit Institution of Belize. The Self-Assessment was conducted applying the SAINT[1] methodology as provided by the Netherlands Court of Audit (NCA) for members of the International Organization of Supreme Audit Institutions (INTOSAI). This tool is applicable to the members of the Latin America and Caribbean Organization of Supreme Audit Institutions (OLACEFS).

The focus of the Self-Assessment was global, with an approach to the whole organization, since representatives from all departments of the SAI of Belize participated.

The basic concepts of 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 can reduce their vulnerability 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 carried out on September 2nd, 3rd, and 4th 2015, in Belize City, Belize, 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 describes 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 gap analysis between the vulnerability profile and the integrity control measures the organisation has in place.

[1] Self-Assessment of Integrity, assessment of the institutional vulnerability and the maturity level of the integrity control systems implemented, applicable to organizations in the public sector.

On the basis of these descriptions, recommendations are formulated for improving the integrity control system.

We would like to acknowledge the kind co-operation we received from the Supreme Audit Institution of Belize to conduct the *IntoSAINT* workshop, especially the efforts of the workshop participants and the coordinators: Miss Maria Rodriguez, Supervisor of Audit and liaison officer to OLACEFS, and Mr. Edmund Zuniga, Examiner of Accounts and *IntoSAINT* moderator.

1 Description of organisational processes

Before the start of the workshop, a pre-selection of key-processes of the Office of the Auditor General of Belize was prepared in cooperation with the moderator of the SAI of Belize. During the workshop, this pre-selection was discussed and the participants confirmed to focus the Self-Assessment on the following processes.

The vital organisational processes involved are:

Primary processes

1. Process audits: financial, compliance and performance (planning, execution, supervision, communication of results of audits).
2. Establishment of administrative individual responsibilities.
3. Generation of reports to Parliament on the inspections carried out.
4. Audit quality control.

Secondary processes

5. Management of human resources (shared responsibility* with recruitment and selection, training, organizational climate, remuneration, personnel management).
6. Financial management (shared responsibility* with finance, treasury).
7. Information management (shared responsibility* with development, maintenance, access of information systems data collection, entry and distribution; electronic process, access to systems development).
8. Management of facilities (catering, equipment).
9. Logistic support (transportation, accommodation).

Management or governance processes

10. Documentation management.
11. Process for the development, processing and approval of institutional standards.
12. Strategic planning (mission, vision, institutional values and strategic objectives).
13. Organizational management: organizational structure, mandate, monitoring, internal audit, telework.
14. Internal control system.
15. Quality management (continuous improvement).

*Shared responsibility with the Ministry of Public Service.

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 Supreme Audit Institution of Mexico have been compared with a list of inherent vulnerabilities, as indicated in the table below.

As shown below, the 15 participants assigned a score to every single inherent vulnerability regarding the relevance of each of them, *vis-à-vis* the list of processes defined for the institution. The scoring ranks from 0 to 3, according to the following criteria:

Score	Relevance
0	Not important
1	Relevant
2	Important
3	Very important

	Vulnerable areas /activities /actions		Average score	Level
Relationship of the entity with its environment	Contracting	procurement, tenders, orders, assignments, awards	**0.73**	**Low**
	Payment	subsidies, benefits, allowances, grants, sponsoring	**0.00**	**Low**
	Granting / Issuance	permits, licenses, identity cards, authorizations, certificates	**0.13**	**Low**
	Regulating	conditions of permits, setting standards / criteria	**0.67**	**Low**
	Inspection / audit	supervision, oversight, control, inspection, audit	**2.80**	**High**
	Enforcement	prosecution, justice, sanctioning, punishment	**0.07**	**Low**

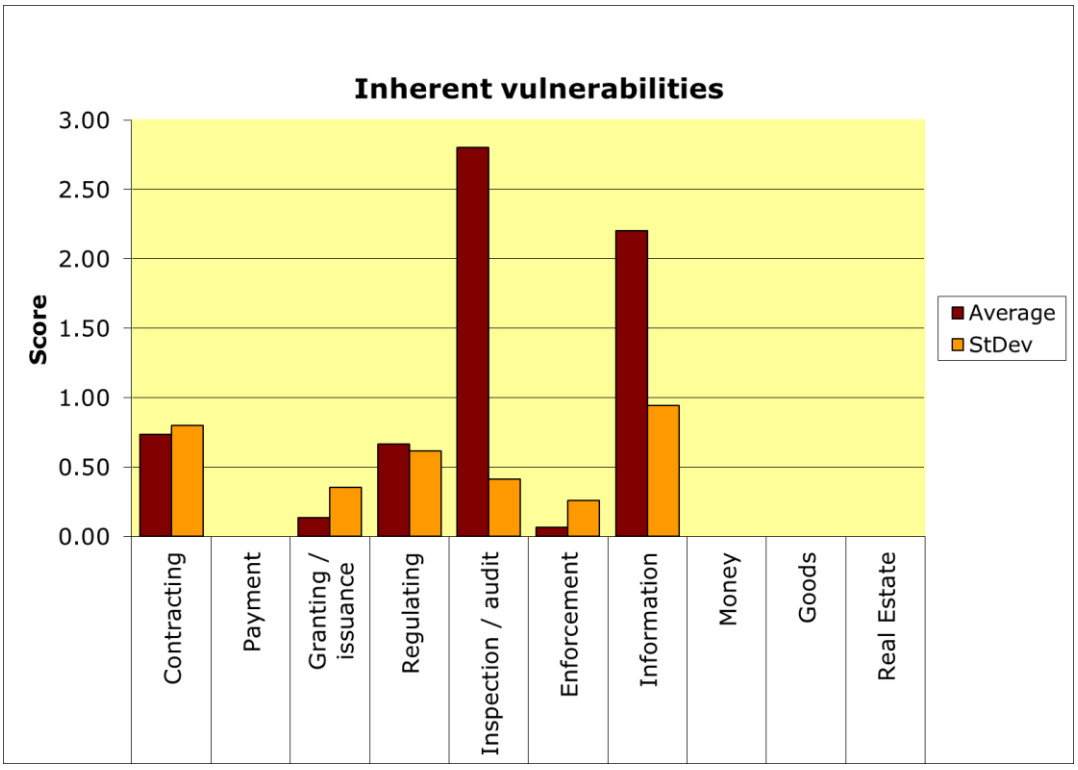
Managing public property	Information	national security, confidential information, documents, dossiers, copyright	**2.20**	**High**
	Money	treasury, financial instruments, portfolio management, cash/bank, premiums, expenses, bonuses, allowances, etc.	**0.00**	**Low**
	Goods	purchasing / selling, management and consumption (stocks, computers)	**0.00**	**Low**
	Real estate	buying / selling	**0.00**	**Low**
			0.67	**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
average > 1,6	High

The scores on the inherent vulnerabilities are represented in the following diagram.



The score assigned by the participants is in red; the standard deviation is in orange, which shows the divergence level in the scores assigned by the participants. The average inherent vulnerability identified during the workshop, applicable to the Supreme Audit Institution of Belize is **0.67**, which is in a **low** level.

From the table and the corresponding diagram, it can be concluded that the most relevant vulnerable areas are:

- **Inspection / audit**
- **Information**

It is worth mentioning that, regarding the mandate of a Supreme Audit Institution, the areas identified above use to rank typically with a high level of inherent vulnerability. Even though "enforcement" uses to be also typical for SAIs, the workshop participants considered that this element was not applicable to the Office of the Auditor General of Belize since the institution is not in charge of the justice management or the application of punishments, as the Judiciary does.

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.

Within the framework of this assessment method, the vulnerability enhancing factors are divided in the following five clusters as a common point of reference:

1. Environment Complexity
2. Institutional Change / dynamics
3. Top Management's attitude
4. Personnel
5. Problem history

During the workshop, the 15 participants evaluated and discussed the full list of vulnerability enhancing factors. They assigned a score to every single factor regarding the real presence of each of them at the Supreme Audit Institution of Belize. The scoring ranks from 0 to 3, according to the following criteria:

Score	Relevance
0	Not important (the situation does not occur)
1	Partially relevant (the situation occurs not often)
2	Important (the situation occurs often)
3	Very important (the situation occurs very often)

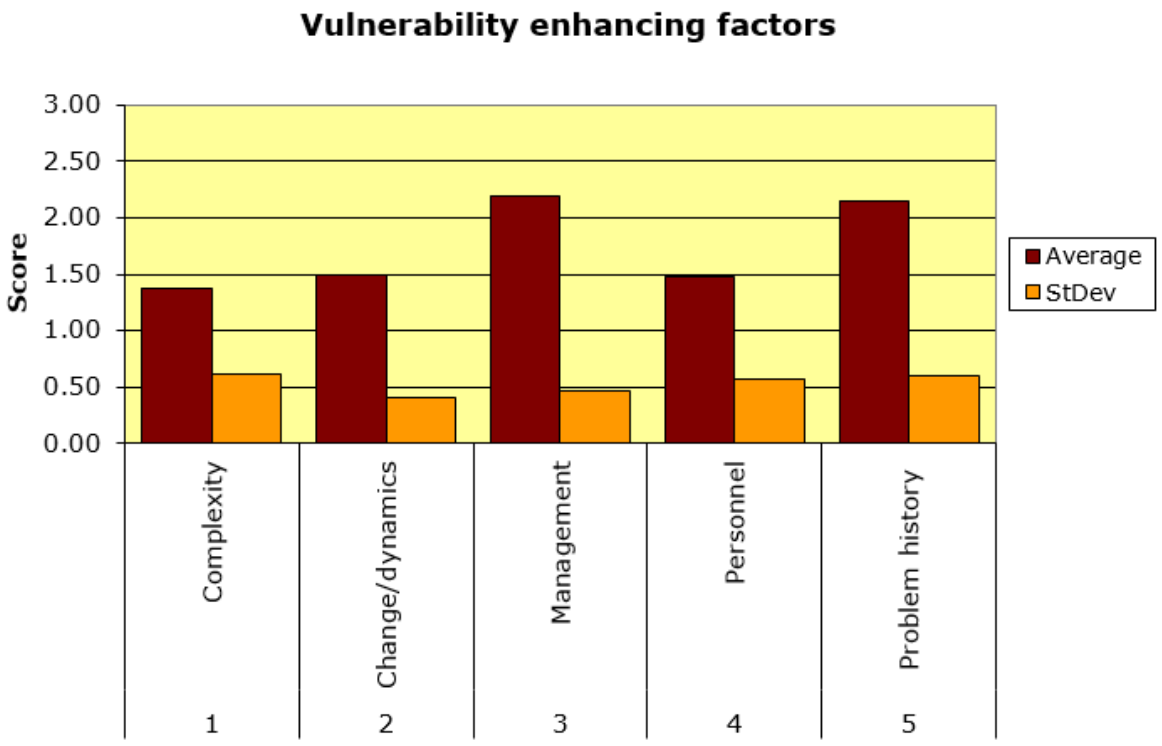
This list and the average score per vulnerability enhancing factor can be found in **Annex 2**. The average scores of the workshop participants per cluster and the resulting level of vulnerability are indicated in the table below.

Clusters of vulnerability enhancing factors	Average score (0-3)	Level
1. Environment Complexity	**1.37**	**Medium**
2. Institutional Change/Dynamics	**1.50**	**Medium**
3. Top Management's Attitude	**2.20**	**High**
4. Personnel	**1.47**	**Medium**
5. Problem history	**2.15**	**High**
Overall average score	**1.74**	**High**

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

The average scores on the clusters of vulnerability enhancing factors can be represented as a diagram as follows.



The score assigned by the participants is in red; the standard deviation is in orange, which shows the divergence level in the scores assigned by the participants. The average vulnerability enhancing factors identified during the workshop, applicable to the Supreme Audit Institution of Belize is **1.74**, which is in a **high** level.

The conclusions based on the scoring results of the participants are shown as follows.

- **Environment complexity**

The workshop participants considered that public sector organizations in general, including SAI of Belize, use to have a lot of **bureaucracy** regarding their operations, which complicate the achievement of institutional objectives. On the other hand, there is a broad perception regarding **external political intervention** in the SAI, especially from legislators. This situation could affect the performance of audits, especially those related to sensitive topics. Finally, there is a perception that a close relationship **(networks of relations)** between SAI's officers and other public organizations (such as the Ministry of Finance) exists, which could damage SAI's objectivity in the discharge of its duties.

- **Institutional change / dynamics**

The SAI of Belize has been affected by **strong downsizing** and by **scarce resources** (human, material and IT) to perform its duties. Regarding human resources, besides lack of personnel, the participants considered that the main problem lies in the way that working teams are structured. For example, the rotation strategy of staff has complicated the continuous work and planning, since new people involved in particulars projects have to start over.

- **Top Management's attitude**

The participants considered that the Top Management at the SAI of Belize is made up by the Auditor General, the Deputy Auditor General and Supervisors of Audit. There is a general perception of a **lack of communication** and **distrust** between the Top Management and the staff which make difficult to propose advice and suggestions. A mutual understanding was found complicated meanly between the staff and Supervisors of Audit, rather than the staff with the Auditor General or the Deputy Auditor General. Some staff considered that Top Management's decisions are based on subjective judgements. For example, some people could be frustrated to no longer carry out their work because of a lack of trust without foundation. Finally, there is a lack of motivation in the staff because sometimes they feel they are not heard.

- **Personnel**

There was a consensus regarding more vulnerability enhancing factors related to the **organizational environment**. Participants considered that **physical working conditions** are not optimal; in addition that there are not civil protection measures (lack of fire extinguishers, emergency plans). Participants recognized that external inspection are carried out, however they are not being effective. On the other hand, there is a perception that the staff have **low professional status and low rewards,** since promotions are not necessarily based on their performance. This situation, besides no access to health care, could affect the risks in the institution in integrity terms. Finally, in spite of the fact that the SAI of Belize has courses, there is not a way to measure knowledge, and the SAI does not have a comprehensive capacity-building strategy according to institutional needs.

It is worth noting that individual factors such as personal debts, having other interest, overspending, personal secrets or threats, and addictions, do not represent a serious risk for the institution.

- **Problem history**

There is a perception of **informal communication (gossips)** in the institution, and a lack of mechanisms to receive advice and suggestions from the staff. In general, there are not many incentives to provide feedback. Because of that, previous problems in integrity matters seem not to be solved over time.

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 **low**.

The level of enhanced vulnerability is **high**.

Together this results in a **MEDIUM** vulnerability profile, as shown in the following table.

Vulnerability profile

Vulnerability enhancing factors / **Inherent vulnerabilities**	Low	Medium	**High**
Low	Low	Low	**Medium**
Medium	Medium	Medium	High
High	High	High	High

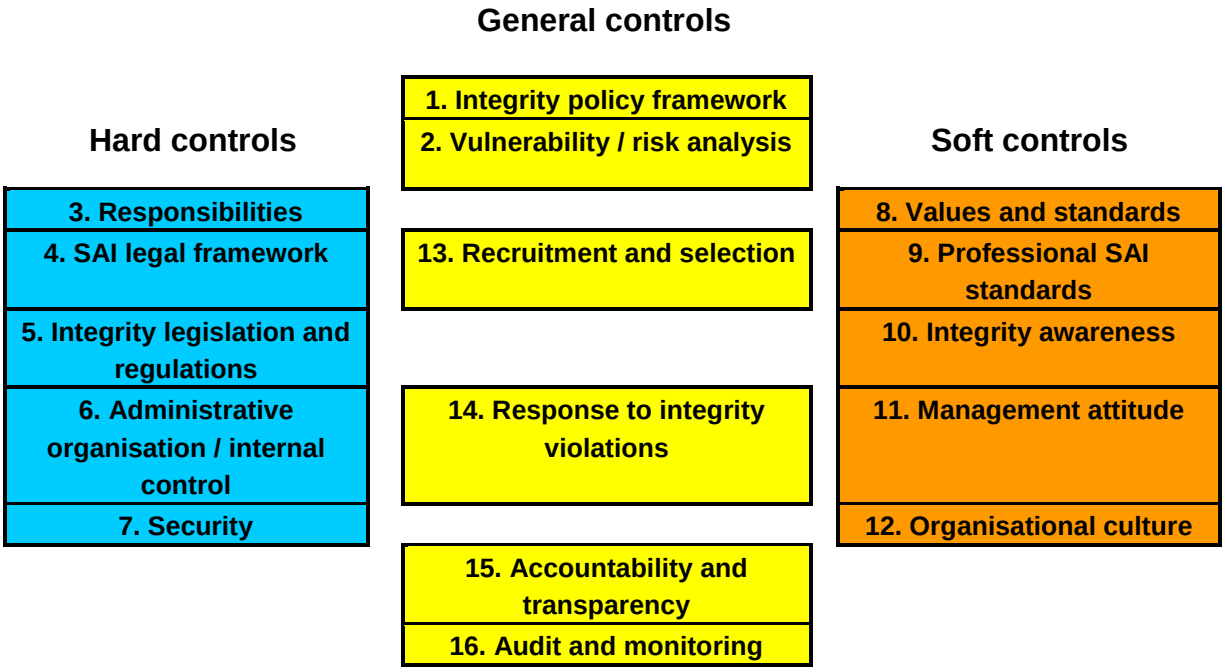
This vulnerability profile is taken into account when comparing this level with the maturity level of the integrity control system and plays a role as part of the gap analysis.

3 Maturity level of the Integrity Control System

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. 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. This set of controls also takes the International Standards for Supreme Audit Institutions (ISSAI) into account, as far as ethical components are involved.

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) and 16 clusters.

The clusters are shown in the model below.



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 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 table below.

Level	Criteria
0 – Low	▪ The measure does not exist, at least to the best of my knowledge
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 outcome of the assessment of the integrity control system is shown below per cluster of measures.

Nr.	Clusters of controls	Average	Level
	General controls	**1.02**	**Medium**
1	Policy framework	1.21	Medium
2	Vulnerability / risk analysis	0.80	Low
13	Recruitment and selection	1.33	Medium
14	Response to integrity violations	1.03	Medium
15	Accountability	1.20	Medium
16	Audit and monitoring	0.56	Low
	Hard controls	**1.52**	**Medium**
3	Responsibilities	0.67	Low
4	SAI legal framework	1.85	Medium
5	Integrity legislation and regulations	1.46	Medium
6	Administrative organisation and internal control	2.01	High
7	Security	1.62	Medium

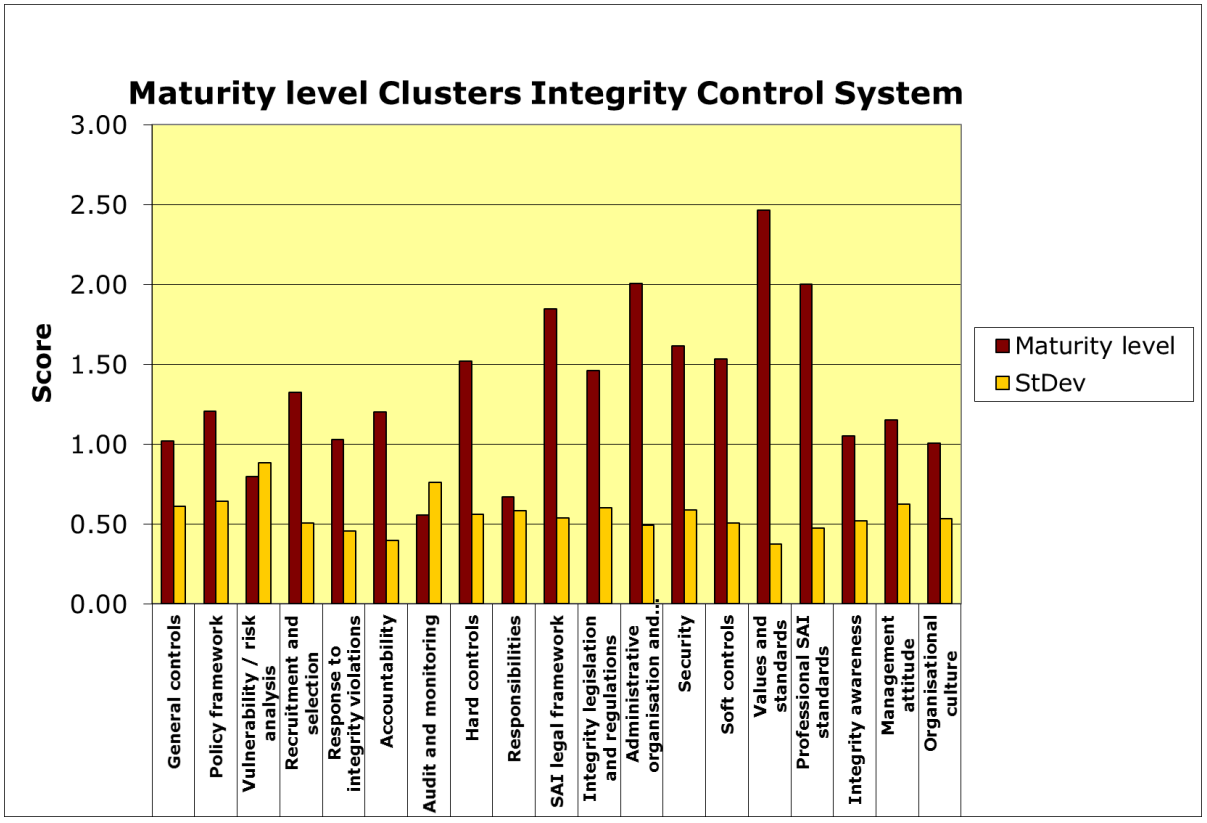
	Soft controls	1.53	Medium
8	Values and standards	2.47	High
9	Professional SAI standards	2.00	Medium
10	Integrity awareness	1.05	Medium
11	Management attitude	1.15	Medium
12	Organisational culture	1.00	Low
	Overall average score of all clusters	**1.34**	**Medium**

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 ≤ x ≤ 1	1	Low
1 < x ≤ 2	2	Medium
2 < x ≤ 3	3	High

For the case of the SAI of Belize, the average is **1.34**. According to the *IntoSAINT* methodology, the maturity level of the integrity control system is **medium**.

The following diagram shows the maturity level of the clusters of integrity controls, as assessed by the workshop participants.



The score assigned by the participants is in red; the standard deviation is in orange, which shows the divergence level in the scores assigned by the participants. 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 in a satisfactory level or did not need improvement, because they do not apply to the situation within the SAI of Belize or would cause too much bureaucracy, relative to their contribution to the integrity control system.

Regarding the results of the graph, the **mean strength** is related to values and standards. On the other hand, the **opportunity areas** are related to the audit and monitoring of integrity, specific responsibilities about integrity, vulnerability / risk analysis and the organizational culture.

The ultimate results from this exercise are reflected in the recommendations formulated in chapter 5.

4 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.

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.

During the workshop, the participants conducted an assessment on the general level of vulnerabilities and resilience. For the SAI of Belize, the workshop established a "balance" between the vulnerability profile (level: **medium**) and the maturity level of the integrity control system (maturity level: **medium**). However, this situation does not mean that the institution is protected against integrity risks. The result implies that there is still room for further improvements, especially regarding the integrity control measures.

Considering the identified vulnerabilities and the maturity level of the integrity control system, the participants formulated recommendations to reduce vulnerability and strengthen controls. Those recommendations are presented on the next chapter.

5 Recommendations

Based on the assessment of the vulnerabilities and the (maturity level of) the integrity control system, the workshop participants formulated 19 recommendations to the Top Management. These recommendations are presented in this chapter and may be clustered by theme as follows.

A. Integrity Policy Framework

1. Design, issue and disseminate an Institutional Integrity Policy, which includes diverse elements such as the Codes of Ethics and Conduct, Guidelines to Prevent Conflicts of Interest, and other kind of regulations in that field. This Policy should be included in the Strategic Plan, get the SAI's staff involved, and should be extended to auditees, suppliers and stakeholders whom the SAI of Belize has a relationship with.
2. Establish formally an Integrity Committee with clearly defined responsibilities in writing, which will be in charge of the institutional integrity management, and will report continuously to the Auditor General about progress in this matter.
3. Appoint an Integrity Counsellor, who will be responsible for the implementation of the Institutional Integrity Policy. The person who holds this position must have high ethical and moral values, and enjoy a great prestige within and outside the institution.
4. Establish an official mechanism to receive staff's complaints and suggestions on integrity matters, in order to analyse and solve them timely. Involved parties should be notified about the whole process of claims and final resolutions.
5. Disseminate the Institutional Integrity Policy to the whole organization in order to sensitize staff on the integrity relevance and all its elements, mechanisms in place, as well as the results to be achieved.
6. Carry out periodic assessments about the efficiency of the elements and actions that make up the Institutional Integrity Policy, and monitor its progress, in order to guarantee its continuous improvement.

B. Internal control framework

7. Establish a comprehensive internal control framework, which harmonizes the isolated procedures and strategies, by getting all staff involved in the organization's governance structure.
8. Perform risk analysis applicable to all processes, activities, positions and areas in the institution.
9. Effectively safeguard information by implementing mechanisms to keep the ownership of data, and avoid a filtering and misuse of information.

C. Prevention

10. Carry out installed-capacity (material, human, financial and all kind of resources) and required-equipment diagnosis for the discharge of the institutional duties, taking into consideration available human resources and the working team structures.
11. Implement civil protection measures among all the staff in order to be prepared before any emergency, having the related protocol knowledge, training and necessary equipment.

D. Organizational environment

12. To the best of the institutional mandate, analyse the possibility to regard health care and other services for the staff in order to guarantee their welfare and their better performance.
13. Implement a strategy to improve the organizational environment of the institution (work climate studies, job satisfaction surveys, recreational events, recognition to workers' good performance, among others) in order to promote trust and a strong commitment to the SAI.

E. Capacity-building and training

14. Design and carry out a comprehensive training strategy, taking into consideration the needs of every single area of the institution, in order to enable staff development and foster professional skills. This training strategy should include integrity matters.
15. Collaborate with international partners (such as INTOSAI, CAROSAI and OLACEFS, among others) to access the best practices in integrity matters, auditing issues and other relevant areas.

F. Leadership

16. In order to develop integrity awareness among staff, it is necessary for management to lead the process.
17. Include the participation of the top management in the institutional training program in order to be more aware on integrity relevance, foster their own skills, and have more elements for the decision-making processes.

G. Communication strategy

18. Implement an effective cross sectional communication strategy, strengthening a top-down and bottom-up approach, in order to promote a respectful relationship and ownership within the institution, as well as to avoid misunderstandings and informal communication.

H. Promotion of good governance

19. To the best of its mandate, consider the convenience for the SAI of Belize to take the leadership of integrity and promote it among the public sector organizations in Belize. This strategy might be an opportunity to position the SAI at the forefront in transparency, accountability and good governance in the Belizean public service, enabling the institution to lead by example.

We believe that the implementation of the recommendations presented in this chapter will contribute to improving the integrity awareness and the integrity control system within the Office of the Auditor General of Belize.

Annex 1 List of participants

1. **Berthalee Parks**, Audit Clerk I, Compliance Audit Unit
2. **Charles Flowers**, Supervisor of Audit, Performance Audit Unit
3. **Cynthia Cayetano**, Examiner of Accounts III, Compliance Audit Unit
4. **Dareth Obermayer**, Examiner of Accounts III, Performance Audit Unit
5. **Eldon Simpson**, Examiner of Accounts III, Compliance Audit Unit
6. **Hubert Humes**, Audit Clerk I, Compliance Audit Unit
7. **Jemma Williams**, Second Class Clerk, Administration/Registry
8. **Jennifer Myvett**, Examiner of Accounts, Performance Audit Unit
9. **Kathia Patt**, Second Class Clerk, Performance Audit Unit
10. **Lovina Martinez**, Audit Clerk I, Compliance Audit Unit
11. **Merli Lopez**, Audit Clerk II, Performance Audit Unit
12. **Sheila Schmidth**, Audit Clerk I, Accounts
13. **Theresita Chun**, Second Class Clerk, Administration/Registry
14. **Tyrone Palmerston**, Audit Clerk II, Compliance Audit Unit
15. **Wilfred Richards**, Audit Clerk II, Performance Audit Unit

Contact person:

- **María Rodríguez,** Supervisor of Audit and liaison officer to OLACEFS.
- **Edmund Zuniga,** Examiner of Accounts and IntoSAINT moderator.

Annex 2 Vulnerability enhancing factors

	Vulnerability enhancing factors	Average	Score
	1 Complexity		
1.1	Innovation / advanced computersystems	0.87	Medium
1.2	Complex legislation	1.27	Medium
1.3	Special constructions (legal / fiscal)	1.27	Medium
1.4	Bureaucracy	2.00	High
1.5	Lobbying	0.80	Low
1.6	Networks of relations	1.53	Medium
1.7	Mix of public-private interests (commerce / competition)	0.87	Medium
1.8	Need for external expertise	1.53	Medium
1.9	Political influence/ intervention	2.20	High
	Average score cluster 1	**1.37**	**Medium**
	2 Change/dynamics		
2.1	Young organisation	1.43	Medium
2.2	Frequently changing legislation	1.20	Medium
2.3	Strong growth or downsizing	1.93	High
2.4	Privatisation, management buy-out	0.33	Low
2.5	Outsourcing	0.60	Low
2.6	Crisis (reorganisation, threats with huge impact, survival of the organisation or job at stake)	2.00	High
2.7	External pressure (pressure on performance, expenditure, time, political pressure, shortages / scarce resources in comparison with duties)	3.00	High
	Average score cluster 2	**1.50**	**Medium**
	3 Management		
3.1	Dominant	2.80	High
3.2	Manipulative	2.73	High
3.3	Formal / bureaucratic	1.73	High
3.4	Solistic operation	1.87	High
3.5	Remuneration strongly dependent on performance	1.73	High
3.6	Lack of accountability	1.53	Medium
3.7	Ignoring advice / signals	2.53	High
3.8	Defensive response to criticism or complaints	2.67	High
	Average score cluster 3	**2.20**	**High**
	4 Personnel		
*	***Work environment/ loyalty***		
4.1	Pressure on performance / income dependent on performance	1.67	High

4.2	Low status / lack of esteem/ low rewards / low career prospects	1.80	High
4.3	Poor working conditions/ high workload	2.33	High
4.4	Group loyalty	2.40	High
4.5	Power to obstruct	1.73	High
*	***Individual***		
4.6	Having other interests (side jobs, etc.)	1.27	Medium
4.7	Personal debts	1.47	Medium
4.8	Lifestyle (overspending)	1.33	Medium
4.9	Personal secrets (vulnerable for blackmail)	0.87	Medium
4.10	Personal threats	0.60	Low
4.11	Addictions (alcohol, drugs)	0.73	Low
	Average score cluster 4	**1.47**	**Medium**
	5 Problem history		
5.1	Complaints	2.33	High
5.2	Gossip and rumours	2.67	High
5.3	Signals / whistle blowers	1.47	Medium
5.4	Earlier incidents (recidivism)	1.67	High
5.5	Administrative problems (backlogs, inconsistencies, extraordinary trends)	2.60	High
	Average score cluster 5	**2.15**	**High**
	Average all clusters	**1.74**	**High**

Annex 3 Integrity control system

Cluster	Measure		Average (0-3)
1		**Policy framework**	
	1.1	Are integrity measures embedded in a systematic policy framework?	1.07
	1.2	Are concrete objectives formulated as part of the integrity system?	1.43
	1.3	Have time and funds been budgeted for implementing integrity measures?	0.87
	1.4	Are integrity measures communicated?	1.27
	1.5	Is integrity policy formally laid down in an overall policy plan?	1.40
		Average cluster score	**1.21**
2		**Vulnerability / risk analysis**	
	2.1	Are general vulnerability / risk analyses regularly carried out?	0.73
	2.2	Are in depth analyses carried out for vulnerable areas and positions?	0.86
		Average cluster score	**0.80**
3		**Responsibilities**	
	3.1	Are (functional) responsibilities assigned for integrity?	0.71
	3.2	Is there systematic consultation between officials responsible for integrity?	0.80
	3.3	Is there an integrity counsellor?	0.20
	3.4	Is there periodic coordination with outside organisations and external stakeholders?	1.13
	3.5	Has someone been appointed to coordinate integrity policy (externally)?	0.50
		Average cluster score	**0.67**
4		**SAI legal framework**	
	4.1	Is the existence and independence of the SAI embedded in the Constitution (ISSAI 10; principle 1)?	1.79
		Is a legal framework 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)?	1.43
	4.3	- a sufficiently broad mandate and full discretion, in the discharge of SAI functions (ISSAI 10, principle 3)?	2.13
	4.4	- unrestricted access to information (ISSAI 10, principle 4)?	2.20

	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)?	1.93
	4.6	- financial and managerial / administrative autonomy and the availability of appropriate human, material and monetary resources (ISSAI 10, principle 8)?	1.60
		Average cluster score	**1.85**
5		**Integrity legislation and regulations**; Are rules in place for:	
		Conflicts of interest	
	5.1	- (rules on) external positions/financial interests?	1.29
	5.2	- (rules on) the acceptance of gifts/invitations?	1.80
	5.3	- (rules on) confidentiality?	2.00
	5.4	- (rules on) preventing "revolving door arrangements"?[2]	0.93
	5.5	- (rules on) external screening of contractors and/or licence applicants?	0.47
	5.6	- (rules on) lobbying?	0.64
	5.7	- (rules on) influence of politicians on civil servants?	1.20
		Integrity within organisations	
	5.8	- (rules on) combating/dealing with undesirable conduct?	1.60
	5.9	- (rules on) expense claims?	2.47
	5.10	- (rules on) email, internet and telephone use?	1.93
	5.11	- (rules on) use of the employer's property?	1.73
		Average cluster score	**1.46**
6		**Administrative organisation and internal control**	
	6.1	Is there a specification of vulnerable activities and positions?	1.20
	6.2	Are specific procedures in place for the conduct of vulnerable activities?	1.07
	6.3	Does everyone have a job description?	2.60
	6.4	Are duties segregated?	2.57
	6.5	Is the "four eyes principle"[3] applied?	2.27
	6.6	Are there mandate regulations?	2.13
	6.7	Is a job rotation scheme in place?	2.21
		Average cluster score	**2.01**
7		**Security**; Have measures been taken with regard to:	
	7.1	physical security (locks, windows, doors, safes, etc.)?	1.50
	7.2	Information security (IT security, clean desk policy,[4] classification of information as confidential/secret, access authorisations, filing	1.73

[2] "Revolving door arrangements" refer to those cases in which a person works for the government, and then works in the private sector or other organizations that look for something from the government (for example: suppliers, consultants, audit firms, etc.).

[3] The "four eyes principle" or "two signatures" prevents staff in certain positions working without supervision, putting at least two people in place to work together, especially in high-risk areas or processes.

		systems)?	
		Average cluster score	**1.62**
8		**Values and standards**	
	8.1	Is integrity part of the organisation's mission?	2.20
	8.2	Have core values been formulated (e.g. impartiality, professionalism etc.)?	2.20
	8.3	Has an (integrity) code of conduct been introduced?	2.53
	8.4	Is an oath or pledge taken?	2.87
	8.5	Is there a special ceremony for taking the oath or pledge?	2.53
		Average cluster score	**2.47**
9		**Professional SAI standards**	
	9.1	Is the SAI 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)?	2.13
	9.2	In working with the executive, do auditors act only as observers and not participate in the decision-making process (ISSAI 11, principle 3, Guidelines)?	2.14
	9.3	Are 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)?	2.07
	9.4	Are 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)?	2.13
	9.5	Does the SAI have 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)?	2.27
	9.6	Have employees been involved in the formulation of the code of ethics and/or the standards with ethical significance?	1.27
		Average cluster score	**2.00**

[4] "Clean desk policies" implies to keep desks and office spaces clean so that unauthorised persons cannot learn anything from open documents.

10		**Integrity awareness**	
	10.1	Is integrity an explicit requirement for all positions?	1.53
	10.2	Are regular training courses given to consider integrity?	0.73
	10.3	Are staff in vulnerable positions informed of particular risks and counter measures?	1.33
	10.4	Do staff get special assistance and/or council to cope with integrity risks?	0.60
		Average cluster score	**1.05**
11		**Management attitude**	
	11.1	Does management actively promote the importance of integrity?	1.20
	11.2	Does management actively seek the implementation of an integrity policy and integrity measures?	1.13
	11.3	Does management always respond appropriately to integrity issues?	1.00
	11.4	Does management itself comply with integrity regulations and/or code of conduct?	1.27
		Average cluster score	**1.15**
12		**Organisational culture**	
	12.1	Is regular attention paid to the importance of integrity?	1.13
	12.2	Can integrity questions be discussed safely?	1.00
	12.3	Is there sufficient opportunity to express criticism?	0.43
	12.4	Is the importance of integrity clearly explained to external relations?	1.00
	12.5	Is there open communication on integrity violations and how they are dealt with?	0.80
	12.6	Is there a culture of holding others responsible for their conduct?	1.67
	12.7	Is there sufficient consideration of job satisfaction?	1.00
		Average cluster score	**1.00**
13		**Recruitment and selection**	
	13.1	Is a fixed procedure in place to deal with all applications?	1.07
	12.2	Is an advisory selection committee consulted?	1.13
	13.3	Are CVs, diplomas, references, etc. always checked?	1.60
	13.4	Are the members and the audit staff of the SAI evaluated (pre-employment screening) on their qualification and moral integrity required to completely carry out their tasks (ISSAI 1: Lima declaration; Section 14.1)?	1.13
	13.5	Is integrity part of the introduction programme for new members of staff?	1.07
	13.6	Where necessary, do staff sign a declaration of confidentiality?	2.80
	13.7	Is integrity periodically considered in work consultation meetings and performance interviews?	1.20
	13.8	Is integrity a specific consideration when hiring temporary and external staff?	1.13

	13.9	Is integrity considered when staff leave or during exit interviews?	0.80
		Average cluster score	**1.33**
14		**Response to integrity violations**	
	14.1	Is a notification procedure in place for employees to report suspected violations ('whistle blowers procedure)?	1.33
	14.2	Are managers accessible by employees to report suspected violations?	1.67
	14.3	Is an integrity counsellor involved in the notification of violations?	0.00
	14.4	Is there a procedure for handling signals and complaints from external sources?	1.07
	14.5	Is there a protocol to investigate integrity violations?	1.27
	14.6	Are integrity violations recorded centrally?	0.40
	14.7	Does the organisation always respond to integrity violations?	1.00
	14.8	Are suspicions of criminal offences always reported to the public prosecutor or the police?	1.13
	14.9	Are incidents evaluated and discussed with staff involved?	1.40
		Average cluster score	**1.03**
15		**Accountability and transparency**	
		General	
	15.1	Does senior management receive reports to account for the integrity policy conducted?	0.00
	15.2	Do staff representatives receive reports to account for the integrity policy conducted?	0.73
	15.3	Do democratically elected authorities (parliament, municipal council, etc.) receive reports to account for the integrity policy conducted?	0.87
	15.4	Are the reports systematically structured and containing clear indicators?	0.00
		SAI specific	
	15.5	Are the SAI's mandate, role, responsibilities, organization, mission, strategies, audit manuals, procedures and criteria public (ISSAI 20, chapter 2/3)?	2.27
	15.6	Are the SAI's audit findings and conclusions subject to contradictory procedures (consultation with the audited entity) (ISSAI 20, chapter 3)?	2.33
	15.7	Are the SAIs accounts public and subject to external audit or parliamentary review (ISSAI 20, chapter 4)?	1.40
	15.8	Is the SAI open about measures to prevent corruption and ensure clarity and legality in its own operations (e.g. disciplinary sanctions) (ISSAI 20, chapter 5)?	1.33
	15.9	Are the status of auditors (magistrates in the Court model, civil servants or others), their powers and obligations public (ISSAI 20, chapter 5)?	1.33

	15.10	Are outsourcing, expertise and sharing audit activities with external entities, public or private, performed under the responsibility of the SAI and subject to precise rules (ISSAI 20, chapter 5)?	1.07
	15.11	Are codes of ethics issued and public (ISSAI 20, chapter 5)?	1.13
	15.12	Does the SAI issue public reports on audit findings, management, performance and communicate openly with the media or other interested parties (ISSAI 20, chapter 6)?	1.93
		Average cluster score	**1.20**
16		**Audit and monitoring**	
	16.1	Is the integrity system periodically audited by an internal auditor?	0.40
	16.2	Is the integrity system periodically reviewed by an external auditor and/or supervisor?	0.60
	16.3	Is the integrity system periodically monitored or evaluated by management?	0.67
		Average cluster score	**0.56**
		Total score = average score of all clusters	**1.34**