MANUAL

Into

Integrity Self Assessment for Supreme Audit Institutions

2013

Contents

Introduction

SAINT stands for Self-Assessment INTegrity. It is a tool originally developed for public sector organisations in the Netherlands, but it has been customised to meet the specific needs of Supreme Audit Institutions (SAIs). This particular version of SAINT is available for members of INTOSAI and is called 'IntoSAINT'. IntoSAINT enables SAIs to assess their vulnerability and resilience to integrity violations. It also yields recommendations on how to improve integrity policies and management. IntoSAINT is a self-diagnosis tool presented as a (two-day) workshop for a group of participants from the assessed entity.

IntoSAINT encompasses a framework of integrity controls. This framework covers relevant International Standards for SAIs regarding integrity and ethical requirements (for example included in ISSAI 11, 30, 40 and 200). IntoSAINT may therefore help SAIs to assess their compliance with these standards in support of the institutional quality of the SAI. It is also possible to apply the instrument within the context of a peer review.[1]

This manual outlines the basic principles of IntoSAINT, considers its components and looks at its design and operation.

This manual consists of two parts:

Part I	Principles of the methodology
Part II	Guidance for application

[1] ISSAI 5600, Appendix, 1.7 Internal governance.

Part I: Principles of the methodology

1 The concept of integrity

Integrity is not a simple concept to define. Many overlapping and distinct definitions are used. The term integrity is derived from the Latin in-tangere, meaning untouched. It refers to virtue, incorruptibility and the state of being unimpaired. Integrity not only refers to the absence of fraud and corruption, but it also entails common decency and proper behaviour. In this way it is a positive and broad concept, that is strongly related to ethical principles and culture. IntoSAINT uses this wide and positive definition of the term integrity.

- *Responsibility for integrity*

Civil servants act with integrity if they observe the values and standards of good administration. Integrity embraces not only the requirements of incorruptibility but also such values as honesty, sincerity, sociability, neutrality, consideration, reliability, customer-focus, respect, objectivity and decency. A civil servant must take care to exercise his responsibilities and use the powers, information and resources at his disposal for the benefit of the public or the general interest he serves and behave correctly with his colleagues and the public.

The same is true of an organisation but an organisation must also do all it can to ensure that its personnel will not succumb to temptation. It should, for example, design processes in such a way that civil servants are not exposed to temptation, not make unreasonable or impossible (conflicting) demands on them, regularly and clearly remind the staff of the importance of integrity, ensure that managers set a good example, and create an open and transparent culture in which criticism is accepted, mistakes can be made and difficult questions can be discussed. In brief, the organisation must implement an effective integrity policy and should apply appropriate ethical standards..

Integrity is therefore a product of good administration and good employment practices. The assessment focuses on integrity risks that might seriously undermine confidence in the organisation and thus in its image and continuity.

- *Precondition for government authority and public confidence*

Integrity is a precondition for the effective and continuous performance of the public sector. A government that lacks integrity loses the confidence of the public and ultimately its authority. The public must be able to trust the government because it is the sole provider of many vital services, such as the issue of passports, licenses and subsidies. Owing to this monopoly and the public's dependence, the government must be unblemished and beyond all suspicion.

- *Integrity: not only laws and rules but also moral responsibility*

Integrity means more than simply observing rules and laws. The law is a lower limit and a minimum moral starting point. Rules and laws cannot cover all situations. The tension is the greatest when rules are lacking or uncertain, such as in new, complex and changing situations. Also civil servants may be confronted with contradicting sets of values. Precisely in such situations, civil servants must be able to form a morally acceptable opinion and act responsibly in accordance with the values and standards of good administration. They must also do so in situations in which they have discretionary powers.

- *Integrity policy: not only repression but above all prevention*

Integrity policy calls for a combination of repression and prevention. On the one hand, an organisation must take measures if its staff act inappropriately (repression). On the other, it must do all it can to remove temptations that might induce civil servants to act inappropriately (prevention). Priority should be given to prevention. Not only is it more effective but on balance the investment is many times smaller than the cost of repairing damage caused by inappropriate behaviour: "an ounce of prevention is worth a pound of care".

- *Integrity policy: not ad hoc but continuous*

The attention paid to integrity must be permanent. If policy is scaled down when things are going well, the risk of incidents increases. In other words, integrity and integrity policy must be permanently embedded in the organisation and be a fixed part of the organisation's operational management and quality management. Integrity cannot be treated as a project because a project ends and is not continuous. Integrity must be a standard component in the management and policy cycle.

The concept of integrity and the different ways of approaching this topic may be illustrated by the following table.

Compliance approach	**Integrity approach**
Negative approach	Positive approach
Rule based: imposed norms (law and regulations)	Principle based: shared norms and values (decency)
Hard controls	Soft controls
Opinion: people are bad	Opinion: people are good
Focus on preventing integrity violations	Focus on facilitating good behaviour
Legal focus	Managerial focus
Repression/Reactive	Prevention/Pro-active

The consensus reached is that a well-balanced mix of both approaches is necessary for good results.

The assessment methodology presented is this manual has adopted the wider scope of integrity as described in this chapter. This scope is more suitable for an instrument that is designed for use in the context of a preventative approach.

- *Integrity and SAIs*

SAIs have an important role to play to strengthen the accountability and transparency, but also the integrity of government and public entities. SAIs should be model organisations through leading by example.[2] Many SAIs acknowledge these principles and reflect this in the formulation of their mission. Various ISSAI standards[3] use the term integrity without providing an exact definition, but it is reasonable to assume that these ISSAIs intend to adopt the wide scope of the integrity concept as IntoSAINT does.

[2] ISSAI X (2): The value and benefits of SAIs – making a difference to the lives of citizens (exposure draft).

[3] For example ISSAIs 30 and 40.

2 Risk Assessment

Risk analysis is a natural reflex in our daily lives. To a certain degree, we are programmed to analyse the risks inherent in every situation. Often we do so subconsciously, implicitly or even intuitively. We know from our own experience that we are almost continuously analysing and weighing up risks. Risk analysis can stop us doing things or change the way we approach them. It makes us more alert so that we can respond more quickly and thus reduce the chance of misadventure. We assess the nature and seriousness of a risk so that we can take measures to avert it or mitigate its consequences.
Such exercises are important to us personally, but they are vital to organisations. All public organisations are vulnerable and are to some extent exposed to integrity risks. Organisations must be aware of their vulnerabilities and risks, so that they can take targeted measures. It is both illusory and undesirable to think that all risks can be averted or closed out. That would need so many rules and procedures that the organisation would no longer be able to function. Risk analysis can help decide what measures will help to reduce the risks for an organisation to an acceptable level.

- *Risks*

In literature a risk is described as the likelihood or probability of a certain undesirable incident occurring multiplied by its impact or the damage it would cause (Risk = Probability x Impact). The formulation of a concrete risk contains: undesired event (actor, action, time and place), the damaged interest and the damage caused.

An undesirable event is something that can happen to an institution, organisation or person and cause damage to a (desired) situation/ position. It is caused by specific circumstances and/or (un)deliberate action.

This damage can take different shapes and therefore pose different types of risks. For instance a political risk may be that a policy will not be accepted by parliament, a performance risk means that the organisation will not reach its objectives, a financial risk that an organisation may lose money. These risks can be the consequence of either changing circumstances, a calamity, acts of people or acts of organisations. The consequences relate to organisations, institutions and/or people.

- *Integrity risks*

An integrity risk is a possible undesirable event that damages the public sector. Damage in the public sector can be defined in terms of financial loss, the impairment of services provided to clients or members of the public, the waste of tax revenue, public loss of respect for or confidence in the government, political and administrative implications or a deterioration in the working atmosphere. The common denominator is that misuse of power damages the image of the public sector and undermines the public trust in and legitimacy of government.

- *Vulnerabilities*

As explained above concrete risks are specifically defined undesirable events, formulated in terms of actor, action, time, place and damage caused. Vulnerabilities are defined on a higher level of abstraction, indicating areas where risks are more likely to occur. It’s useful to

focus on vulnerabilities, because it provides a good insight into potential problems and the ways to address them, without having to define all possible risks in detail.

From research, professional knowledge and experience it is known that some areas of activity in the public sector produce more integrity risks than others. These are inherently vulnerable processes or functions. Processes in which there is intensive contact with "clients" (members of the public or businesses) are more vulnerable to violations, because there are more opportunities and temptations. The same is true of processes that involve valuable public assets.

In addition to the characteristics of public sector activities, certain circumstances may increase vulnerability to integrity breaches. These so called "vulnerability enhancing circumstances or factors" are not integrity risks in themselves but they may 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.).

Examples of these vulnerability enhancing factors are complicated legislation, external pressure and low employee loyalty.

Together the inherently vulnerable areas and the vulnerability enhancing factors constitute a 'vulnerability profile' for an organisation, entity or process.

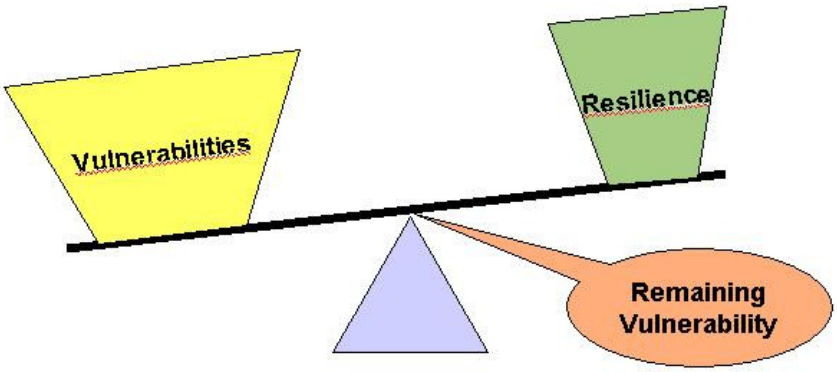
- *Reducing vulnerability and risk mitigation*

Organisations may cope with their vulnerability 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 will rarely be possible. 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. Since vulnerabilities are diverse in their nature it is important to design a well-balanced set of controls or integrity control system. Depending on the 'maturity level' of the integrity control system the organisation is more or less resilient to the vulnerabilities it is facing.

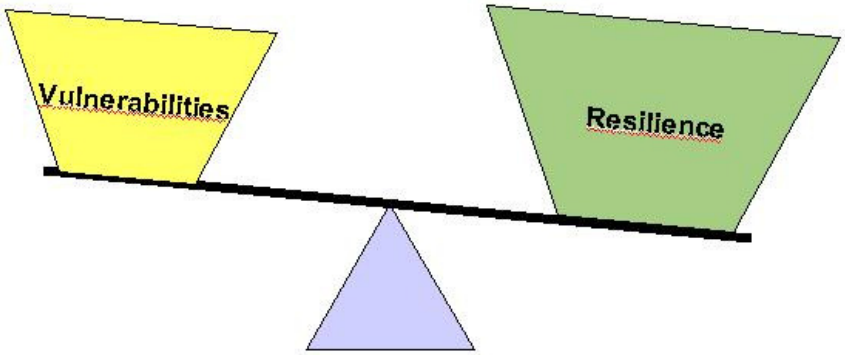
The relationship between vulnerabilities and controls may be illustrated by the following diagrams picturing a balance or set of scales.

The first diagram shows a situation in which the resilience is not fully balancing the vulnerabilities. This implies that there is still remaining vulnerability, indicating there is still room for further improvements.



The next diagram shows the situation that vulnerabilities and resilience are more or less in balance. However it may still be desirable to (further) reduce the level of vulnerability or to strengthen the maturity level of the integrity controls, because there may be unacceptable vulnerabilities or weaknesses in the integrity control system.

The final diagram shows another possible situation, but one that is not very likely to occur in real life. It illustrates the importance of a well-balanced approach, because an excessive implementation of integrity controls to counter vulnerabilities must also be avoided.



3 Basic principles

The methodology described in this manual is focussed on the assessment of:
- integrity vulnerabilities and risks ;
- the maturity level of the integrity control system.

The basic principles and features are described in this chapter of the manual.

- *Targeted at prevention*

The assessment method is targeted at prevention. It is not designed to detect integrity violations or to punish (repress) unacceptable conduct. The method is designed to identify the main integrity weaknesses and risks and to strengthen the organisation's resilience with a view to preventing future violations.

- *Approach: Self-assessment*

IntoSAINT is designed as a self-assessment tool. It is a self-diagnosis tool presented as a two-day workshop for 15 to 20 participants. Self-assessment means that the organisation itself tests its resilience to integrity risks. The assessment draws on the knowledge and opinions of the staff. This approach is based on the belief that the staff has the best insight into the potential weaknesses, risks and maturity of the organisation's integrity measures. The organisation reveals its own weaknesses and the staff make recommendations on how to strengthen resilience.
To avoid misunderstandings among participants it is important to stress the self-assessment concept of IntoSAINT. It has to be absolutely clear to all participants that IntoSAINT is neither an audit approach, nor a training course. It should also be clear that IntoSAINT is focussed on the SAI itself and not on its auditees.

- *The workshop moderator*

The workshop is presided over by an experienced moderator. His/her role can best be described as that of a process supervisor. The moderator leads the participants through the various steps in the workshop and shows them how to identify the main vulnerabilities and risks and how to formulate recommendations to strengthen the integrity management system in order to eliminate or minimise vulnerabilities and risks.

- *Learning to think in terms of vulnerability and risk*

The assessment method promotes thinking in terms of vulnerability and risk. During the assessment, the participants identify the main vulnerabilities and risks and then make recommendations on how to minimise them. Thinking in terms of vulnerability and risk is a specific skill that has to be learnt to formulate a balanced integrity policy. If an organisation has relatively little experience in this area, the assessment may serve as a first introduction. The lessons learnt can therefore be replicated to improve the organisation's approach to integrity.

- *Insight into the integrity control system*

The assessment method not only identifies integrity vulnerabilities but also focuses on the organisation's resilience to integrity violations. For a number of integrity measures is evaluated whether they have been introduced, whether they are being implemented and observed and whether they are effective or not. This produces a good insight into the

maturity of the integrity control system and the organisation's resilience to integrity violations. The measures can be divided into three broad categories:
(1) hard controls consisting of rules, procedures and the design of administrative systems and internal controls;
(2) soft controls targeted at behaviour, culture and management attitude;
(3) general controls having a broader scope and/or impact, for example the organisation of integrity policy.

- *Concrete management report/action plan*

The end product of the assessment is a concrete management report/action plan.[4] This report explains to management where measures must be taken to strengthen the organisation's resilience to integrity violations. Focusing attention on these specific issues adds to the general integrity policy.

- *Raising general integrity awareness*

Apart from providing a concrete insight into integrity vulnerabilities and weaknesses and making recommendations to strengthen resilience, the assessment can significantly increase the awareness of integrity. Taking an intense and collective approach to the issue, like in the self assessment, focuses the participants' minds on why integrity is so important. The participants' collective discussions of the importance and significance of integrity before, during and after the workshop are of great value. The participants pass on their findings throughout the organisation.

[4] A template for this report is available in the workshop material.

4 Outline of the assessment method

The assessment methodology consists of five separate steps:

(a) Analysis of object and its processes
The first step is to define the *object* of the assessment and to analyse the relevant *processes*. The object may be the entire SAI or organisational entities of the SAI. For the selected object a list of primary, secondary and management & control processes has to be drawn up. The quality of the list will determine the further course of the assessment. As well as being complete, the list must indicate the processes so that they are recognised and understood without being overly detailed. Cryptic names lead to uncertainty and should be avoided.

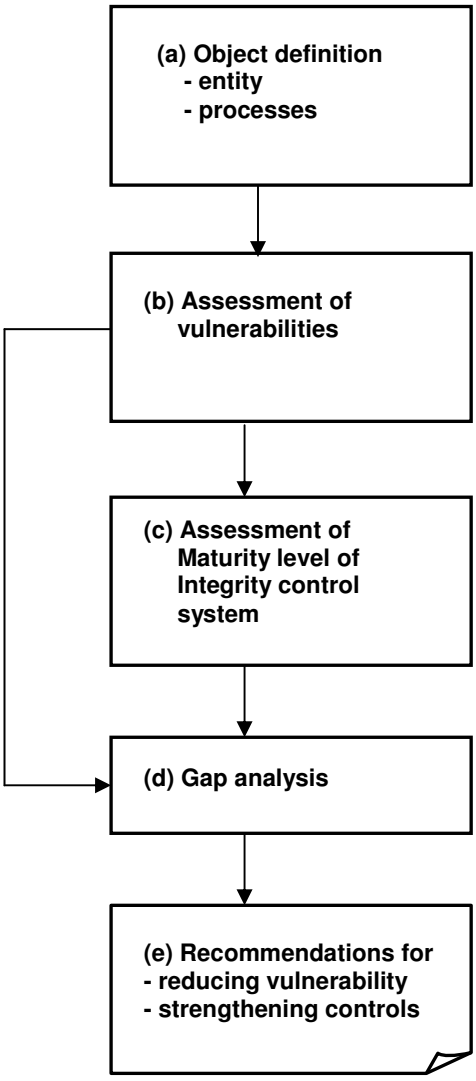
(b) Assessment of vulnerabilities
In this step, an estimate is made of the *vulnerability*, i.e. the potential exposure to integrity violations, of the processes named in step (a). This step consists of four sub-steps:
1. relating the list of processes to an overview of processes in the public sector that are known to be vulnerable to breaches of integrity;
2. considering the presence or absence of vulnerability enhancing factors;
3. producing an overview and overall assessment profile of the perceived vulnerability;
4. Indicating the most vulnerable processes.

(c) Assessment of the maturity of the integrity control system
In this step the participants assess the maturity of the integrity measures that together form the organisation's *integrity control system*. The system is divided into 16 clusters, with the clusters being subdivided into three blocks (general, hard and soft controls). This module consists of the following steps:
1. brief introduction to the integrity control system, made up of measures, clusters and categories;
2. brief introduction to the maturity levels;
3. assessment of the maturity level of all the measures by awarding them points;
4. summary of the scores to produce an average per cluster and block; this shows which clusters and blocks are relatively robust or weak.

(d) Gap analysis
This module reveals the link between the vulnerabilities (b) and the maturity level of the integrity controls (c). The analysis should clearly show whether the overall level of vulnerability is in balance with the maturity level of the integrity control system. The gap analysis is intended to discover options to reduce vulnerabilities and to strengthen integrity controls.

(e) Management report and recommendations
Steps (a) to (d) will provide input for the assessment report.
The central question is which measures are the most appropriate to make the most vulnerable processes more robust. The results of this exercise form the input for the assessment report and for the recommendations to strengthen resilience against integrity risks.

The following diagram presents a schematic overview of the assessment methodology.



Part II: Guidance for application

5 Preparation

This chapter provides guidance and explanations for the moderator of a self-assessment workshop. The moderator is the expert leading the workshop (preferably together with an assistant), but he/she is also the person responsible for preparing the workshop carefully and summarising the results in an assessment report afterwards.

Apart from the guidance in this chapter of the manual, a toolkit is available, including slide-show presentations and a spreadsheet to support the moderator and the workshop participants in implementing the assessment method.

- *Co-ordination*

Before the start of the self-assessment a number of actions need to be taken and preconditions need to be fulfilled. The assumption is that there will be someone from within the SAI who will act as a co-ordinator and contact person for the assessment. This may be someone from an operational or supporting staff unit, who should be in the position to communicates easily with the moderator and within the SAI.

- *Management support*

The first step is to obtain support from management. Sometimes management has taken the initiative for the assessment, but it can also be the initiative of the audit department or an external party. It is important that management acknowledges that integrity is a management responsibility. The scope of the assessment should be clear to and supported by management.

- *Object selection*

The second step is to decide what the object of the assessment will be. Usually this is the SAI as a whole, but it may also be a specific unit. The management responsibility should be clear and preferably management should be involved in the object selection. It is important to make an inventory of the relevant processes before the workshop takes place. At the beginning of the workshop, the participants will be shown the list and asked whether corrections or additions should be made (see chapter 6).

- *Selection of participants*

The third step is to select a group of employees who are familiar with the unit and/or processes that are to be assessed. For practical reasons the group should be no larger than 20 persons. It is important that participants feel free to express their opinions and experiences. Therefore it is advisable to avoid a combination of a subordinates and superiors in the same group. Participation should be on a voluntary basis.

- *Planning*

The workshop itself will take two days, including an introduction session. It is important that the group can spend these days undisturbed, so an external location is ideal.
During the introduction session there is time to explain the objective and nature of the self-assessment and discuss the concept of integrity. It is important that the participants understand that the workshop is focussed on what they can tell about integrity risks and the resilience against integrity violations. Also confidentiality should be stressed.

- *Interaction*

It is important to have free discussions during the workshop. Discussion will make the results more robust. It also contributes to raising awareness. The moderator plays a vital role in facilitating the group discussions. He or she should not only have the necessary knowledge of the tool, but also well-developed facilitating skills and an open attitude. A way to stimulate discussion is to work in couples or small groups during the steps of the workshops.

- *Reporting*

A reporting model (format) is available that can be used during and after the workshop, so the preparation of the management report does not require a lot of extra work. The presentation of the results to management should cover the vulnerabilities, integrity control system and remaining risks. The focus should be on improvements and recommendations: the 'action agenda'.

To raise awareness in the entire organisation, communication is vital. The intention to perform a self-assessment and the results of the workshop and action agenda should be widely communicated within the organisation.

6 Definition of object and processes

6.1 Introduction

In this part of the workshop the following questions are essential:

1. Is the entire SAI or part of it going to be evaluated?
2. What tasks are being performed by the (relevant part of the) SAI?
3. What organisational processes are vital?

The assessment is focussed on the key processes of an organisation or organisational entity. The object of the assessment should be well-defined and clearly linked to management responsibility.

The identification of processes is a key part of the assessment methodology. This step must be prepared before the workshop takes place. Most organisations have only a limited number of core processes. To identify these processes, the relevance for the organisation and their use of resources have to be considered. Core processes are often related to the (legal) duties of the organisation. Interviews with management and staff will also help to identify what processes are considered important or even vital for the organisation. The list of processes should be complete but not too detailed. The list should be formulated in such a way that everyone understands and recognises the relevance of the processes.

The moderator walks through the prepared list of processes with the group of workshop participants and makes sure this is the complete list of primary, secondary and management processes that contribute together to the vital tasks of the organisation or organisational entity. It is recommended to limit the number of processes to approximately 15 to 20 processes to avoid too much detail. At the start of the workshop the moderator will ask the participants to agree with the list of pre-selected processes, if necessary after implementing some modifications

The conclusions of this step are entered into the management report.

The processes can be categorised as follows:

- *primary processes;*
- *secondary processes;*
- *management and control processes*.

The assessment should concentrate on vulnerable *primary and secondary* processes. By their nature, management and control processes are less vulnerable, but in some cases they should be considered.
When the assessment is applied to an *organisational unit* of the SAI (e.g. a particular department), it will usually suffice to consider the primary and secondary processes only. The selection of processes should consider only those processes (or sub-processes) that actually take place within the unit.
When the assessment is applied to the entire SAI the management and control processes are of interest and should be included in the assessment.

The following sections provide background information and further details on the various types of processes (primary, secondary and management and control) typical for SAIs.

6.2 Primary processes

The primary processes are the organisation's core processes. A primary process can be defined as "a method to convert resources (money, people, information, etc.) into products and services that achieve the organisation's tasks and goals". There is no generally accepted classification of primary processes. They are highly specific to the type of organisation.

Taking into account the existing knowledge of the nature of SAIs and the processes within SAIs, the following pre-selection can be made of relevant primary processes for most SAIs.

- Monitoring the audit environment (for example: information gathering and communication with stakeholders);
- Audit processes (planning, execution, reporting, issuing audit opinions, archiving, communication, quality control, follow up etc.);
- Development processes (developing methods, capacity building etc.);
- International activities (for example: conducting international audits, maintaining institutional relationships and contributing to international training events).

6.3 Secondary processes

A secondary process can be defined as "a process that directly or indirectly facilitates the primary processes". For use by SAIs we have classified the secondary processes as follows:

- Personnel (human resource) management;
- Financial management;
- Information management;
- Facility management.

By way of illustration, these processes are divided into subsidiary processes below. We would stress, though, that the SAI itself must classify its own subsidiary processes.

1. Personnel (human resource) management:
   a) recruitment and selection;
   b) training;
   c) remuneration;
   d) working conditions / health and safety.
2. Financial management:
   a) budgeting;
   b) accounting;
   c) fund management.
3. Information management:
   a) development of information systems;
   b) maintenance of information systems;
   c) accessibility / continuity of information systems;
   d) data collection, entry, storage and distribution.

4. Facility management:
    a) housing;
    b) procurement of goods and services;
    c) IT equipment and facilities;
    d) transport.

6.4 Governance processes

Governance processes are closely related to management and control processes.

There are many definitions on internal management and control.

Internal management can be defined as "the process of steering an organisation so that it achieves the policy goals set for it". At an organisation level, it involves:
1) the design of the organisational structure;
2) the design and implementation of the planning cycle at strategic, tactical and operational levels;
3) communication with external parties.

Internal control can be defined as "the process of introducing and implementing a system of measures and procedures to determine whether the organisation's performance is and will remain in agreement with the plans and corrective measures agreed to achieve the policy goals". At an organisation level, it involves:
1. risk analysis and management;
2. internal controls;
3. internal communication of the effect of internal controls;
4. periodic progress checks in response to management reports and follow-up measures/changes;
5. monitoring the proper operation of the internal control system.

For SAIs important governance processes are related to for example:
- *Strategy*: formulating mission and (long term) strategy, programming audits and other activities, communication strategy, relations management;
- *Organisation management*: organisational structure, mandates, supervision, internal audit;
- *Auditor General / Board level*: Appointment and remuneration of the Auditor General or Board members, relation management etc.

7 Assessment of vulnerabilities

7.1 Introduction

This part of the workshop focuses on the vulnerability profile, answering the following questions:

- What are inherent vulnerabilities?
- Which vulnerability enhancing factors apply?
- What is the overall vulnerability profile?

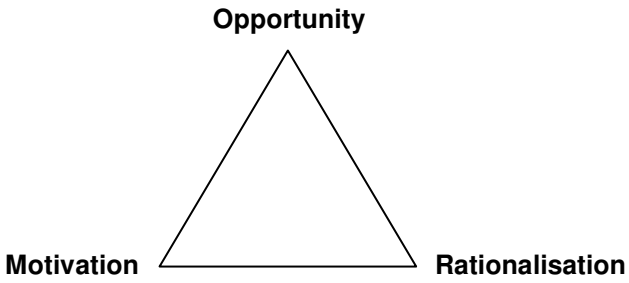
The vulnerability profile is assessed through a number of separate sub-steps. First the organisations inherent vulnerabilities and vulnerability enhancing factors are considered. Then the level of vulnerability is assessed, using a scoring model. Although in general the level of vulnerability is difficult to estimate and may have subjective elements, this methodology provides a relatively simple and objective approach, categorising the level of vulnerability as low, medium of high. The inherent vulnerabilities and the vulnerability enhancing factors constitute together a 'vulnerability profile'. The results of this assessment are entered into the management report.

7.2 Vulnerabilities and temptations

Most civil servants who commit an integrity violation did not intend to do so when they first entered the service. Many succumb to the temptations they face within the organisation. The temptations might be tangible (money, privilege) or intangible (status, recognition, protection). There are also "reverse temptations" such as threats and blackmail. The greater the temptation, the more likely we are to succumb. Wherever possible, temptations should be reduced or eliminated or civil servants should be protected from temptation.

Giving in to temptation must never be tolerated. Civil servants are personally responsible for their actions. By looking upon a violation as a "succumbing to temptation", it is clear what direction preventive measures should take. To a large degree, violations can be avoided if the temptations are removed. A key aspect of risk analysis is therefore to identify the temptations. Risk analysis not only reveals how staff can damage the organisation but also identifies weaknesses in the protection offered by the organisation.

Within the context of fraud prevention, a well-known concept is the so called fraud triangle.



Opportunity refers to the possibility to commit fraud. This possibility must exist for fraud to occur. Therefore removing the opportunity is a strong preventative measure. Motivation is related to the temptation or perceived pressure to commit fraud. As mentioned above it may be possible to identify temptations and to remove them. Finally rationalisation is the argumentation a fraudster has built up for himself to explain why his behaviour is justified under the given circumstances. For an organisation it is possible to have influence on this justification process. For example a rationalisation may be that the culture in the organisation is a justification for fraud or corruption. If the organisations has invested a lot in awareness and culture programs, this argument will fail and potential fraudsters will be more inclined to be loyal to the organisation.

During the workshop the participants will explore the opportunities within their organisation that may lead to temptations (inherent vulnerabilities). An important part of this analysis is exploration of the conditions for possible motivation and justification (rationalisation) which may lower the threshold for integrity violations (vulnerability enhancing factors).

7.3 Assessment of inherent vulnerabilities

Some functions or processes in the public sector are more vulnerable to integrity violations than others. These are inherent vulnerable processes or functions. For instance procurement or granting of subsidies are more vulnerable to breaches of integrity than teaching or archiving.

These vulnerable processes are summarised in the table below.

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

Processes that have one or more of these characteristics are vulnerable to integrity violations. The left-hand column contains two characteristic elements that must be borne in mind when assessing vulnerability. Processes in which there is intensive contact with "clients" or external relations prove to be more vulnerable to incidents because there are more opportunities and temptations. Clients may have considerable (financial) interest in the activities or services of the government. This implies that the temptation may exist to bribe civil servants or to manipulate government decision making in a favourable way for the client. It also creates temptations for civil servants to accept or to ask for favours.

Managing public property is also a vulnerable area. Valuable property is vulnerable to theft or loss. This includes not only money, goods or real estate, but also information as a valuable public asset.

Explanation per inherent vulnerability

Contracting

This involves mainly public procurements for goods and services. This type of activity makes the government vulnerable to fraud, corruption, conflicts of interest and unfair competition.

Payment

The public sector does payments for various reasons, for example subsidies, grants, (social) benefits and allowances. This creates a vulnerability, because payments may be done to recipients who are not entitled to them. There is a risk of fraud, corruption or conflicts of interests. Not only the procedures to establish the eligibility for payments are vulnerable, but also the payment processes themselves.

Granting / Issuance

By law or regulation the government has the duty to grant or issue licenses, permits, passports, identity cards etc. This may be so important for individuals or companies that it may provoke undue influence (bribing for example) on civil servants, if it is foreseen that the

license or permit for example will not be granted otherwise. This vulnerability increases if the salaries of civil servants are relatively low in comparison with the value of the licenses and permits.

Regulating
Setting standards and formulating conditions are government activities that may be vulnerable to lobbying and undue influence. Companies for example may benefit a lot when standards are favourable for them and unfavourable for competitors. In this respect the vulnerability of 'regulating' is comparable with 'granting/issuance'.

Inspection / Audit
Inspections and audits are usually conducted by government to protect vital interests, for example to protect public safety or financial interests. The results of inspections and audit may have considerable impact on those involved. Inspectors and auditors are therefore vulnerable to undue influences. They may be tempted to limit the scope of their inspections and audits or to issue a more favourable opinion.

Enforcement
The public sector has unique duties and responsibilities to enforce laws and regulations. This includes for example investigations, prosecution and sanctioning. Obviously this has a considerable impact on those involved and civil servants executing these duties may be under pressure or be subject to temptations. These processes are vulnerable to manipulation or conflicts of interest, but also to intimidation or undue influence. The fact that enforcement has to deal with criminals and others that do not abide by the law, increases the exposure to vulnerabilities.

Information
In executing its duties the government obtains, processes and supplies information, including sensitive information about for example security threats, defence, taxes and health care. Partly this concerns secret or confidential information. Unauthorised disclosure of such information might cause damage to the interests of the government and to the interest of those involved. Keeping databases and processing information are therefore vulnerable activities. Civil servants having access to sensitive information may be corrupted to provide this information to people that are not entitled to it. Confidential information about companies may be used for trading (with insider knowledge) at the stock exchange or abused to gain competitive advantage.

Money
Processes involving the handling or custody of money have a high vulnerability to fraud. This applies to cash money, bank accounts and some short term financial assets, like receivables. Money is generally more vulnerable than goods, because money can be spent immediately for all kinds of purposes. Goods are not always easy to transfer into money. It requires selling of goods or property, which usually means that third parties have to be involved.

Goods

Because of the scale of its activities, the government consumes and manages substantial volumes of goods, for example computer equipment, inventory and vehicles. Managing valuable goods is vulnerable to integrity breaches, especially goods that are easy to trade (for example computers and telephones). Selling government property may create the risk that property is sold for too low a price, due to manipulation by the buyer.

Real estate

The government owns or uses land, buildings and public infrastructure. In almost all cases this involves substantial financial interests. Buying, selling and managing real estate is usually in the hands of only a small group of specialised civil servants. This makes real estate processes vulnerable to fraud, corruption and conflicts of interest.

To assess the level of inherent vulnerability the workshop participants match the list of organisational processes with the list of inherently vulnerable areas and check which vulnerabilities are present. The extent of vulnerability depends on the importance of the processes for the SAI. If the process represents a core activity, is more frequently executed and/or requiring more resources, it is more important for the SAI. In that case a matching inherent vulnerability should score higher. It has to be stressed that the assessment asks for an opinion about the actual situation within the SAI. IntoSAINT moderators have to be aware that participants sometimes tend to refer to their individual notion of the theoretical level of inherent vulnerability of certain types of processes, without realising that they are asked to assess actual processes within their SAIs. Also moderators have to make sure that participants are completely focussed on assessing their own organisation and do not refer to the situation within the public sector in general or auditees. Finally it is essential that participants do their scoring without taking into account the possible effects of controls that might be in place. The methodology asks for an assessment of the *inherent* vulnerability and not for an assessment of the net remaining vulnerability. The difference may be illustrated by the following equation: inherent ('gross') vulnerability minus (effect of) controls equals remaining ('net') vulnerability. It is important that this concept is clear to all participants, since IntoSAINT considers the effect of integrity controls separately (see chapter 8 of the manual).

The extent of vulnerability is indicated using the following scoring method

Score	Importance for SAI processes / activities
0	Not important
1	Relevant
2	Important
3	Very important

The level of inherent vulnerability may be low, medium or high, based on the criteria, explained in paragraph 7.5.

The result is entered into the management report.

7.4 Vulnerability enhancing factors

In addition to a function or process's characteristics, certain circumstances or factors may increase 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.).

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

1. Complexity
2. Change / dynamics
3. Management
4. Personnel
5. Problem history

Per cluster examples of vulnerability increasing circumstances/factors may be identified as in the table below.

1. Complexity
Innovation / advanced (computer) systems
Complex legislation
Special constructions (legal / fiscal)
Bureaucracy
Networks of relations
Lobbying
Political influence / intervention / assignments
Mix of public-private interests (commerce / competition)
Need for external expertise
2. Change/Dynamics
Young organisation
Frequently changing legislation
Strong growth or downsizing
Privatisation / Management buy-out
Outsourcing
Crisis (reorganisation, threats with huge impact, survival of the organisation or job at stake)
External pressure (pressure on performance, expenditure, time, political pressure, shortages / scarce resources in comparison with duties)
3. Management
Dominant
Manipulative
Formal / bureaucratic
Solistic operation
Remuneration strongly dependent on performance
Lack of accountability
Ignoring advice / signals

Defensive response to criticism or complaints
4. Personnel
Work environment / Loyalty
Pressure on performance / income dependent on performance
Low status / lack of esteem / low rewards / low career prospects
Poor working conditions / High workload
Group loyalty
Power to obstruct
Individual
Having other interests (side jobs etc.)
Personal debts
Lifestyle (overspending)
Personal secrets (vulnerable for blackmail)
Personal threats
Addictions (alcohol, drugs)
5. Problem history
Complaints
Gossip and rumours
Signals / whistle blowers
Earlier incidents (recidivism)
Administrative problems (backlogs, inconsistencies, extraordinary trends etc.)

Many of the above mentioned 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. In general it is important to stress that the factors that will be scored should be related to the factual situation of the SAI.

Per cluster the following additional explanation may be provided.

Complexity
Complex structures and systems are not transparent and provide opportunity for fraud. Also in complex environments it is easier to conceal fraud or suppress signals revealing integrity breaches. Complex legislation is about the laws regulating (the work of) the SAI itself. Bureaucracy is about the internal procedures and regulations. Lobbying, political influence or private sector interventions should be scored regarding their possible influence on internal procedures and behaviours.

Change/dynamics
Changes in an organisation or in the environment of an organisation may give rise to instability of the organization. As in case of complexity this may result in opportunities for fraud. Changes and dynamic environments may also lead to uncertainty, dissatisfaction and frustration among employees, providing incentive or rationalisation for fraud or other integrity breaches. Young organization refers to the time of existence of the organization itself, not to the average age of its staff members.

Management
The attitude and behaviour of management ('tone at the top') may increase vulnerability, because of its influence on the organisational culture. In addition it may harm the organisation's resilience against integrity breaches, if managers do not pay proper attention to necessary controls or do not apply control measures to themselves. Who is seen as management depends on the object of the self-assessment: the SAI or one of the Sais units.

Personnel
Various circumstances within an organisation negatively impact personnel loyalty. This may provide motive for fraud or other integrity breaches. Also individual circumstances not directly related to the organisation (for example personal lifestyle or addictions), may provide incentive for integrity breaches.

Problem history
If an organisation has a problem history, it appears that relatively often problems tend to occur again. In many cases integrity breaches point at more structural weaknesses existing in an organisation or in the sector in which the organisation operates. Also existing weaknesses in controls and organisational culture are difficult to fix. In many cases organisations do not learn enough from incidents in the past.

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.

The relevance for each vulnerability enhancing factor is assessed using the a similar scoring model as for the inherent vulnerabilities. The workshop participants estimate the degree of relevance of each factor by awarding 0, 1, 2 or 3 points. The group decision will be reached by computing the average of individually awarded points and group discussion. Next the average score per cluster is computed. Finally the result of this process is entered into the management report.

During the group-discussions on the scores moderators should ask for specific examples that underpin the scores. This will be helpful when formulating the recommendations.

7.5 Assessment of the vulnerability profile

The results of the previous steps (the scoring of inherent vulnerabilities and vulnerability enhancing factors) are summarised in a 'vulnerability profile' for an organisation or organisational entity.

First the average level of inherent vulnerability is computed and next the average level of the clusters of vulnerability enhancing factors. For the inherent vulnerability, as well as the vulnerability enhancing factors, the assessment makes use of the following criteria to determine the level of vulnerability.[5]

Average score	**Level**
average ≤ 0,8	Low

[5] The criteria are based on pilot benchmarks and have no theoretical background.

0,8 < average ≤ 1,6	Medium
average > 1,6	High

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 Vulnerability profile is determined on the basis of the following table.

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

Looking at this table it is important to note that vulnerability enhancing factors may only contribute to a higher level of vulnerability. The overall level of vulnerability is never lower than the level of inherent vulnerability.

The vulnerability profile is incorporated in the management report.

8 Maturity level of the integrity control system

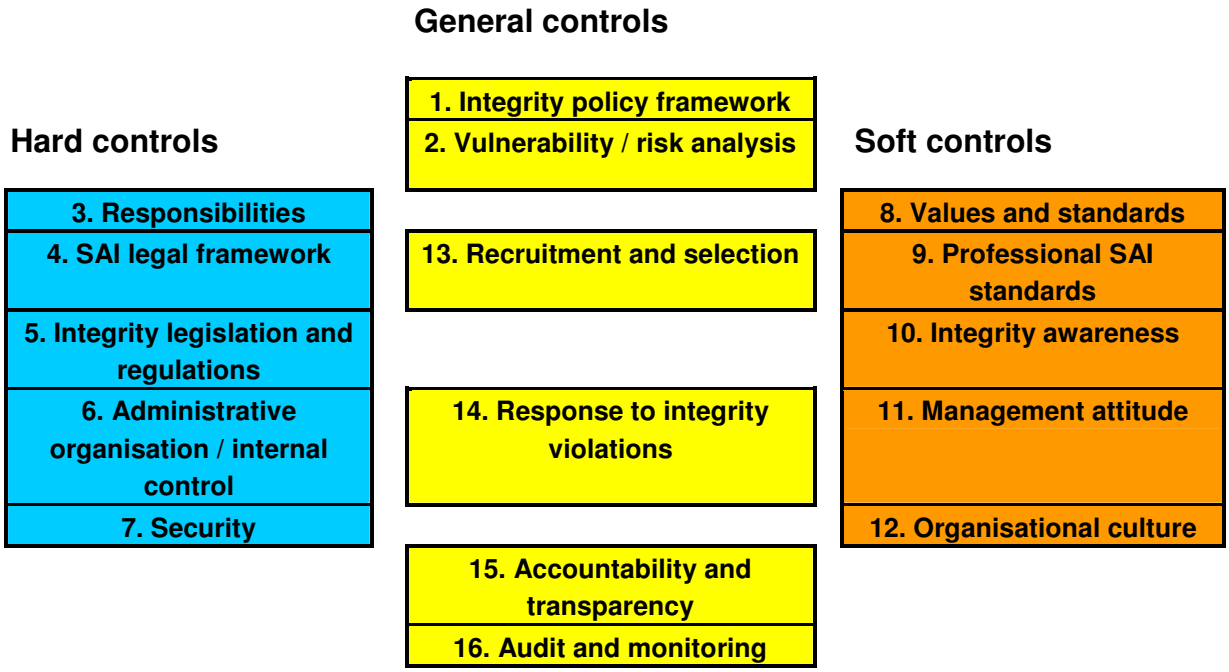
8.1 Introduction

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 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.

8.2 Clusters of measures

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.

Each cluster is described individually below. A brief description, key questions and notes are provided for each cluster. A complete list of all measures is provided in the annex of this manual.

8.3 Detailed description of the clusters of the integrity control framework

1. Integrity policy framework

1.1 Description
Integrity management must be based on policy, and integrity policy (like every other policy) should follow the steps of the policy cycle. The cycle begins with the formulation of a vision and goals and ends when the policy is evaluated and consequently revised where necessary. To formulate a policy framework for integrity, management must first develop a clear vision of integrity and set a clear direction for the measures to be taken. The policy framework must also ensure that the design and implementation of integrity measures are and remain balanced and coherent. The elements or steps that make up the policy framework are considered below.

1.2 Key questions
- Are integrity measures embedded in a systematic policy framework?
- Are concrete objectives formulated as part of the integrity system?
- Have time and funds been budgeted for implementing integrity measures?
- Are integrity measures communicated?
- Is integrity policy formally laid down in an overall policy plan?

1.3 Notes
Policy framework
Integrity measures should be embedded in a systematic policy framework. Since integrity is important to the organisation, senior management must develop a coherent vision of integrity and agree principles. The vision and principles are translated into policy and laid down in a formal document (integrity policy plan). With regard to its scope, the policy should be applicable across the organisation (integral). In practice, however, policy is sometimes limited to personnel management and certain aspects of integrity management, such as security, do not receive the attention they deserve. The influence exerted by the organisation's environment should also be reflected in the policy. Policy should therefore be directed both internally and externally.

Concrete goals
Integrity becomes a concrete policy theme when goals are set. To steer the policy, the goals must meet certain criteria:
- Specific (concrete and targeted);
- Measurable (expressed in verifiable terms);
- Agreed (acceptable to the parties concerned);
- Realistic (feasible);
- Time-bound (deadlines are set);
- Consistent (the goals are not contradictory).

Name activities and resources

Policy goals can be achieved only if action is taken and measures are implemented. Resources (human, material, financial) are needed to take action and implement measures. It must also be clear who is responsible for achieving the goals.

Communication of policy
To be effective, the policy must be known. Many tools and communication channels can be used to disseminate policy and make it known, for example brochures, seminars and the intranet.

Formal integrity policy
To provide an appropriate foundation for integrity management the integrity policy should be formally laid down and accepted.

2. Vulnerability / risk analysis

2.1 Description
A vulnerability analysis entails a systematic analysis of actions, processes and positions that are exposed to possible integrity violations.

2.2 Key questions
- Are general vulnerability / risk analyses regularly carried out?
- Are in depth analyses carried out for vulnerable areas and positions?

2.3 Notes
General vulnerability / risk assessments
All organisations in the public sector are exposed to integrity risks. A general assessment of vulnerabilities and risks is useful to identify integrity risks in general. To address these vulnerabilities an organisation has to make sure that a baseline of integrity controls is in place.

In depth vulnerability / risk assessments
Some processes and positions have a higher integrity risk because certain work areas or circumstances increase their vulnerability to integrity violations. The factors that increase risk must be known so that it can be decided which integrity management measures should be taken to offset the higher risk. This enhances the quality of the process from an integrity position. The vulnerability analysis consists of an assessment of:
- vulnerable operations, activities and actions;
- circumstances that increase the organisation's vulnerability to integrity violations.

3. Responsibilities

3.1 Description
To embed integrity management in an organisation, the responsibilities of the various positions and position-holders must be clear. If they are not, it will be uncertain who is involved in integrity management and who is responsible for it. Responsibilities should be placed with the regular functions in the organisation but it might also be necessary to create specific integrity management positions that have their own powers and responsibilities (counsellors, security officers, integrity coordinators, etc.).

3.2 Key questions

- Are (functional) responsibilities assigned for integrity?
- Is there systematic consultation between officials responsible for integrity?
- Is there an integrity counsellor?
- Is there periodic coordination with outside organisations and external stakeholders?
- Has someone been appointed to coordinate integrity policy (externally)?

3.3 Notes

Responsibilities for internal integrity and internal coordination

Various positions are involved in integrity management within an organisation, for example:

- management (senior and middle management);
- financial and economic affairs;
- personnel department;
- facility services;
- administrative/legal affairs;
- public relations;
- inspection, control and audit departments.

Special positions can be set up within an organisation to deal with integrity issues (these are dedicated integrity positions), for example:

- security officer;
- compliance officer;
- integrity coordinator.

Such positions allow more systematic attention to be paid to integrity than if it were just part of another position. The function and responsibilities of each position should be clear and they should be coordinated through structured consultation in order to prevent shortcomings and duplications.

Integrity counsellors

Integrity counsellors should be appointed so that the organisation's staff can talk to an expert and trustworthy person, seek advice on integrity issues and report integrity violations. In addition to a general integrity counsellor, special counsellors may be appointed for:

- whistleblowers (as part of a scheme to report misconduct);
- sexual harassment/discrimination.

Coordination and responsibility for external integrity relations

Integrity is important not only within the organisation but also in its relations with external organisations. There should be, for example:

- coordination and consultation with other organisations;
- screening of external relations.

Someone should be responsible for these relations.

4. SAI legal framework

4.1 Description

The integrity of the SAI and its independence and impartiality are essential conditions in order to fulfil the duties of the SAI effectively and appropriately.
It is therefore logical that in many countries these conditions are safeguarded in the law or even in the constitution. SAIs are considered to play a vital role in the integrity system within a country, being part of the necessary checks and balances in the public sector. This also requires a solid legal framework. Some of the International Standards of Supreme Audit Institutions (ISSAI) provide guidelines for an appropriate legal framework.

4.2 Key questions

- Is the existence and independence of the SAI embedded in the Constitution (ISSAI 10; principle 1)?

Is a legal framework in place to guarantee:

- 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)?
- a sufficiently broad mandate and full discretion, in the discharge of SAI functions (ISSAI 10, principle 3)?
- unrestricted access to information (ISSAI 10, principle 4)?
- 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)?
- financial and managerial / administrative autonomy and the availability of appropriate human, material, and monetary resources (ISSAI 10, principle 8)?

4.3 Notes

Although the key questions are mostly self-explanatory, it is useful to add some additional guidance provided by ISSAI 11.
ISSAI 11 provides the following guidelines for some of the principles mentioned in ISSAI 10.

Principle 4 (Unrestricted access to information): SAIs should have adequate powers to obtain timely, unfettered, direct, and free access to all the necessary documents and information, for the proper discharge of their statutory responsibilities.

Principle 5 (The right and obligation to report on their work): SAIs should not be restricted from reporting the results of their audit work. They should be required by law to report at least once a year on the results of their audit work.

Principle 8 (Financial and managerial/administrative autonomy and the availability of appropriate human, material, and monetary resources): SAIs should have available necessary and reasonable human, material, and monetary resources. The Executive should not control or direct the access to these resources. SAIs manage their own budget and allocate it as appropriately.

5. Integrity legislation and regulations

5.1 Description

Certain integrity rules are applicable specifically to public sector organisations. These are hard controls that all members of staff must observe. In effect, they are minimum standards. The precise regulations vary from one part of the public sector to another but some of the more common standards and rules are summarised below.

5.2 Key questions

Are rules in place (whether embedded in legislation or regulations) for:

Conflicts of interest

- external positions/financial interests?
- the acceptance of gifts/invitations?
- confidentiality?
- preventing "revolving door arrangements"?
- external screening of contractors and/or licence applicants?
- lobbying?
- influence of politicians on civil servants?

Integrity within organisations

- combating/dealing with undesirable conduct?
- expense claims?
- email, internet and telephone use?
- use of the employer's property?

5.3 Notes

The main regulations are considered briefly below. Criminal law aspects, such as the punishment of civil servants involved in bribery and embezzlement, are not considered. This legislation is applicable, however, to integrity violations.

Conflicts of interest

External positions/interests

If a member of staff is engaged in paid or unpaid activities outside the civil service, for example in industry or sport, there might be a conflict of interest. Depending on the nature of the activities, the staff might be obliged to report them. There should certainly be a duty to report the activities if they are related to the department's work or if there is a connection with the civil servant's own position. Such activities should therefore be reported if there is a relationship between the external activities and the position or the department's activities in so far as they affect the civil servant's performance. If external activities are reported, they should also be registered. For some positions in the public sector, for example in the judiciary, regulations might be in place that require external positions to be made public.

Financial interests and security transactions

A civil servant might have a financial interest in a company that is associated with his position or he might wish to buy or sell securities in such a company. To prevent undesirable conflicts of interest, such interests must be regulated within the public sector.

Gifts/invitations/benefits

A business relation might offer a civil servant something such as a bottle of wine, an invitation to dinner or an admission ticket to an event. The giver might want to thank or influence the civil servant, improve the relationship, or expect something in return. Accepting

a gift might therefore be an integrity risk. A gift should not be accepted unthinkingly and sometimes it should be refused. Above all, a civil servant must not compromise his independence.

Confidentiality/freedom of expression
Many civil servants have access to personal information on members of the public or information that might be of interest to an external party. It goes without saying that such information should be dealt with confidentially and should not be used for personal gain. However, civil servants also have a right to freedom of expression, provided they do not undermine their performance or that of the public sector. A civil servant's fundamental right to freedom of expression is not absolute. It is limited by the assurances required regarding his performance and that of his department. Any comments he makes should be judged in part on the distance between him and the policy on which he comments, the nature of the comments and the way in which he expresses his opinion. Comments can be judged only after they have been made.

Revolving door arrangements
A revolving door arrangement is one in which a civil servant is engaged by a ministry immediately or shortly after he has left employment to carry out the same work, for example through an external consultancy. Such arrangements quickly raise suspicions of favouritism, unfair competition or the semblance of a conflict of interest. They therefore represent a threat to the integrity of the public sector. To prevent them, regulations can be introduced to stop a department engaging a civil servant as an external consultant within a given number of years of his leaving the service.

Screening external relations
Public authorities are required by law to reject applications for grants or licences or withdraw them if a punishable offence might be committed or if it is thought that the recipient will commit an offence. Under the law, a public authority may also decide not to award certain contracts or to cancel them if a company no longer satisfies the requirements of reliability.

Lobbying
Private sector organisations may have special interests to influence opinions or decisions of politicians and/or civil servants. To avoid undue influence by lobbyists regulations may be issued to promote transparency.

Influence of politicians on civil servants
Integrity in the pubic sector requires appropriate relations between politicians and civil servants. Regulations may be issued to protect civil servants against undue influence from politicians.

<u>Integrity within organisations</u>
Undesirable conduct
Civil servants should be respectful and take the opinions, views and efforts of others seriously. Respect is shown through good working relations, team spirit, openness and client-focus. Staff should work without making a distinction on the grounds of religion, faith, political orientation, race, sex or other personal characteristics. Insults, discrimination, sexual

harassment and bullying are forms of undesirable conduct and show a lack of respect for others.

Expense claims
If civil servants incur expenses in the performance of their duties they can reclaim them from their employer. Every organisation has its own rules on expense claims. Since expense claims are very susceptible to fraud, they must be handled carefully. The amount claimed and the reason for incurring the expense must be itemised. Vouchers in the form of bills, receipts and transport tickets should be submitted and the claim should be approved by a superior before being made payable.

Use of telephone, internet and email facilities
Members of staff can send and receive emails and use the internet during working hours using the systems provided by the employer for business purposes. Limited private use of the systems may be permitted provided it does not disrupt the work or is not prohibited. It is technically possible to record (log) the staff's use of the email and internet systems. This provides an insight into an individual's and the department's use of the systems and might also detect misuse.

Use of the employer's property
During working hours the staff inevitably make use of the organisation's assets, such as telephones, computers, printers, fax machines, vehicles and photocopiers. They should treat them with care and avoid damaging them. Time is also an asset and the staff should use it effectively and efficiently. In general, assets should be used for business purposes only and not privately. If assets are also used away from the work location, for example at home, they should still not be used for private purposes. An exception to this rule is possible if only very limited private use is made of an asset. Additional "house rules" may be applicable within the organisation.

6. Administrative organisation / internal control

6.1 Description
The administrative organisation and internal controls are designed to control processes and generate reliable information (complete, accurate and valid) on them. Although the administrative organisation is not exclusively and specifically directed at integrity, many of its procedures and controls are concerned with integrity. It is therefore important that the administrative organisation and internal controls are optimally designed for integrity purposes with a view to prevention (e.g. removing temptation), detection (e.g. revealing stock losses) and repression (e.g. identifying perpetrators). The notes below consider how the administrative organisation and internal controls can promote integrity.

6.2 Key questions
- Is there a specification of vulnerable activities and positions?
- Are specific procedures in place for the conduct of vulnerable activities?
- Does everyone have a job description?
- Are duties segregated?
- Is the "four eyes principle" applied?
- Are there mandate regulations?
- Is a job rotation scheme in place? (ISSAI 40, 6b, element 2)

6.3 Notes

Specification of and procedures for vulnerable activities and positions

Organisations should specify what activities and positions are considered to be relatively vulnerable and requiring more protection to prevent integrity violations. Procedures should be built into the administrative organisation specifically for vulnerable operations and activities, such as collection, contracting, payment, enforcement and licensing. Activities that involve information, money or goods are particularly vulnerable.

Job descriptions

A job description is a document that sets out the content of a particular job. It explains what the job entails and what activities accordingly do or do not form part of the work. If staff do not know precisely what is expected of them, they will be more vulnerable. They should know what they have to do, how they are expected to do it and what responsibilities and powers they have. Vague and uncertain job descriptions give staff a great deal of freedom of action without definite limits. Clear and complete job descriptions provide clarity on the tasks and powers. Clear job descriptions are therefore a precondition for integrity. Job descriptions also give the organisation's management an insight into the vulnerable activities that are carried out by a particular person. The requirements to be satisfied include:

- job descriptions must be drawn up for all members of staff;
- each member of staff must be given a copy of his job description;
- job descriptions must be up to date and describe all activities that have to be performed;
- job descriptions must clearly explain the limits of the powers and responsibilities.

Segregation of duties

Segregation of duties means that vulnerable activities are split up into a series of sub-activities to prevent too many powers and responsibilities being concentrated in one person. There are risks if the duties performed in the conduct of a vulnerable process are not segregated. Activities that form part of such processes are vulnerable if one and the same person always carries them out. The person who considers an application for a licence, for example, should not check whether the licensing conditions are being observed. Duties are adequately segregated if:

- the organisation clearly understands which activities and functions are vulnerable;
- the vulnerable sub-activities are carried out by different people;
- vulnerable activities that cannot be split up into sub-activities and cannot be carried out by several people, are carried out by a team.

Four eyes principle

This measure prevents staff in certain positions working without supervision. In high-risk areas or processes, at least two people should work together. This is known as the "four eyes" or "two signatures" principle. Examples include key management for a safe and the opening of proposals.

Mandate regulations

Mandate regulations lay down the financial and other powers of a particular position. They can set limits, for example, on the assumption of financial commitments or the execution of payments.

Job rotation
To prevent an organisation becoming too close to a particular business relation (e.g. a client or supplier), job rotation schemes should be in place for the staff. After a certain period, members of staff should change job and no longer have any contact with their previous relations. If job rotation is prevented by, for example, the staff's specific expertise, the supplier or client group can be changed. Staff who perform the same work for a long period of time can become vulnerable. There is a danger of undesirable routines creeping in and relations being established with, for example, clients, suppliers and interested parties. The staff may favour a particular client and take too much account of its interests. A job rotation system can prevent this. With a view to integrity, job rotation is particularly important with regard to very vulnerable activities.

7. Security

7.1 Description
Security plays an important role in protecting an organisation's integrity. Security, like the integrity policy in general, must be thoroughly thought out so that the organisation enjoys the protection it deserves. For integrity purposes, both physical security (locks, safes, etc.) and information security (computer access) are of great importance.

7.2 Key questions
Have measures been taken with regard to:
- physical security (locks, windows, doors, safes, etc.)?
- information security (IT security, clean desk policy, classification of information as confidential/secret, access authorisations, filing systems)?

7.3 Notes
Physical security
Physical security is achieved through locks, windows, doors, compartments, passes, safes, etc. to prevent unauthorised persons entering the building. Such measures include unbreakable screens for staff working at counters. In exceptional situations, for example when staff might be threatened, personal security guards may be necessary. Physical security also includes measures for the secure protection of valuable objects, such as money, goods, equipment and documents.

Information security
Information security comprises physical and logical computer security measures. Physical security relates, for example, to access to rooms in which computers are used. Logical computer security is part of the system software and includes:
- identification (who is trying to access the system?);
- authentication (is the person logging on the person he claims to be?, established by means of passwords or biometric identification such as fingerprints);
- authorisation (linking the person to the rights in the system).

These elements of logical computer security must be properly regulated in order to prevent confidentiality and privacy violations and also to limit opportunities for fraud.

Specific elements of information security in relation to integrity include:
- Clean desk policy: Desks and office spaces must be kept clean so that unauthorised persons cannot learn anything from open documents.

- Classification of information as confidential or secret: Documents and files should be classified by their confidentiality and procedures should be in place on how to handle classified information.
- Filing systems: Strictly controlled filing systems should be in place to make sure that confidential and classified information is not accessible for unauthorised persons.

8. Values and standards

8.1 Description

The concept of integrity is closely associated with values and standards. An act's integrity can be measured by its compatibility with the system of values and standards prevailing in the organisation. The values must be meaningful to the organisation and the standards should be universally acknowledged. The values and standards should be incorporated in the mission and laid down in the code of conduct. When a new civil servant takes an oath or pledge, he should be informed and made aware of the values and standards applicable within the organisation.

8.2 Key questions

- Is integrity part of the organisation's mission?
- Have core values been formulated (e.g. impartiality, professionalism etc.)?
- Has an (integrity) code of conduct been introduced?
- Is an oath or pledge taken?
- Is there a special ceremony for taking the oath or pledge?

8.3 Notes

Mission (relationship with integrity)

Every organisation should be able to define its own specific objectives and purpose, i.e. its mission. Since the purpose of a public organisation is invariably to serve the public interest, the mission statement should not only consider the objectives and purpose but also set the parameters within which they can be achieved. Integrity is one of the most important parameters. Integrity should be part of the mission so that there is no doubt about its fundamental value and central importance. Anchoring integrity into the mission focuses minds on the importance of integrity and makes it easier to conduct integrity policy.

Core values and code of conduct

Codes of conduct provide both an overview and a description of the organisation's abstract core values and the concrete standards and rules based on them. Codes of conduct provide the staff with practical guidance and are a benchmark for best practice in the civil service. If members of staff face an integrity problem, the code should help them exercise their own judgment and arrive at a well-founded decision. All civil servants should be involved, directly or indirectly, in the process of drafting the code of conduct.

Oath/pledge

Civil servants hold a special position in society and are part of a government organisation whose purpose is to serve the public interest. Civil servants have exceptional powers and work with public funds. Strict demands are therefore made on the integrity of the people working in the public sector. Although everyone must observe the law and should know that fraud and corruption, for instance, are punishable, civil servants who take an oath or a pledge undertake to honour the Constitution and all other laws and to act "as befits a good

civil servant". They are thus made aware of the responsibilities attaching to their positions and swear or promise to adhere to the values and standards.

The value of taking the oath/pledge is enhanced when embedded in a specific ceremony in which the importance of integrity is stressed. This would also allow top management of the entity to show that it believes integrity is a precondition for trust in the organisation.

9. Professional SAI standards

9.1 Description

Due to the specific nature of SAIs and the importance of independent government auditing, it is very important that SAIs and their staff maintain the highest standard of ethical conduct. This does not only require a firm legal framework (see cluster 4 of the integrity control system), but also general attention within the SAI for appropriate values and standards. These values and rules should continuously be promoted and reinforced in order to influence staff to behave correctly. Various ISSAI standards[6] provide guidance on professional ethical standards.

9.2 Key questions

- 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)?
- In working with the executive, do auditors act only as observers and not participate in the decision-making process (ISSAI 11, principle 3, Guidelines)?
- 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)?
- 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)?
- 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)?
- Have employees been involved in the formulation of the code of ethics and/or the standards with ethical significance?

9.3 Notes

To explain (the background of) the key questions mentioned above reference is made to the relevant ISSAI standards 30, 40 and 200.

[6] ISSAI 11, 30, 200

ISSAI 30: Code of ethics

Chapter 1: Concept, Background and Purpose of the Code of Ethics

2. A Code of Ethics is a comprehensive statement of the values and principles which should guide the daily work of auditors. The independence, powers and responsibilities of the public sector auditor place high ethical demands on the SAI and the staff they employ or engage for audit work. A code of ethics for auditors in the public sector should consider the ethical requirements of civil servants in general and the particular requirements of auditors, including the latter's professional obligations.

4. Due to national differences of culture, language, and legal and social systems, it is the responsibility of each SAI to develop its own Code of Ethics which best fits its own environment. Preferably these national Codes of Ethics should clarify the ethical concepts. The INTOSAI Code of Ethics is intended to constitute a foundation for the national Codes of Ethics. Each SAI has the responsibility to ensure that all its auditors acquaint themselves with the values and principles contained in the national Code of Ethics and act accordingly.

5. The conduct of auditors should be beyond reproach at all times and in all circumstances. Any deficiency in their professional conduct or any improper conduct in their personal life places the integrity of auditors, the SAI that they represent, and the quality and validity of their audit work in an unfavourable light, and may raise doubts about the reliability and competence of the SAI itself. The adoption and application of a code of ethics for auditors in the public sector promotes trust and confidence in the auditors and their work.

6. It is of fundamental importance that the SAI is looked upon with trust, confidence and credibility. The auditor promotes this by adopting and applying the ethical requirements of the concepts embodied in the key words Integrity, Independence and Objectivity, Confidentiality and Competence.

Trust, Confidence and Credibility

7. The legislative and/or executive authority, the general public and the audited entities are entitled to expect the SAI's conduct and approach to be above suspicion and reproach and worthy of respect and trust.

8. Auditors should conduct themselves in a manner which promotes co-operation and good relations between auditors and within the profession.

9. The legislative and/or executive authority, the general public and the audited entities should be fully assured of the fairness and impartiality of all the SAI's work. It is therefore essential that there is a national Code of Ethics or similar document which governs the provision of the services.

Chapter 2: Integrity

12. Integrity is the core value of a Code of Ethics. Auditors have a duty to adhere to high standards of behaviour (e.g. honesty and candidness) in the course of their work and in their relationships with the staff of audited entities. In order to sustain public confidence, the conduct of auditors should be above suspicion and reproach.

13. Integrity can be measured in terms of what is right and just. Integrity requires auditors to observe both the form and the spirit of auditing and ethical standards. Integrity also requires auditors to observe the principles of independence and objectivity, maintain irreproachable standards of professional conduct, make decisions with the public interest in mind, and apply absolute honesty in carrying out their work and in handling the resources of the SAI.

Chapter 3: Independence, Objectivity and Impartiality

14. Independence from the audited entity and other outside interest groups is indispensable for auditors. This implies that auditors should behave in a way that increases, or in no way diminishes, their independence.

15. Auditors should strive not only to be independent of audited entities and other interested groups, but also to be objective in dealing with the issues and topics under review.

16. It is essential that auditors are independent and impartial, not only in fact but also in appearance.

17. In all matters relating to the audit work, the independence of auditors should not be impaired by personal or external interests. Independence may be impaired, for example, by external pressure or influence on auditors; prejudices held by auditors about individuals, audited entities, projects or programmes; recent previous employment with the audited entity; or personal or financial dealings which might cause conflicts of loyalties or of interests. Auditors have an obligation to refrain from becoming involved in all matters in which they have a vested interest.

18. There is a need for objectivity and impartiality in all work conducted by auditors, particularly in their reports, which should be accurate and objective. Conclusions in opinions and reports should, therefore, be based exclusively on evidence obtained and assembled in accordance with the SAI's auditing standards.

19. Auditors should make use of information brought forward by the audited entity and other parties. This information is to be taken into account in the opinions expressed by the auditors in an impartial way. The auditor should also gather information about the views of the audited entity and other parties. However, the auditors' own conclusions should not be affected by such views.

Political Neutrality

20. It is important to maintain both the actual and perceived political neutrality of the SAI.

21. It is important that where auditors undertake, or consider undertaking, political activities they bear in mind the impact which such involvement might have - or be seen to have - on their ability to discharge their professional duties impartially. If auditors are permitted to participate in political activities they have to be aware that these activities may lead to professional conflicts.

Conflicts of interest

22. When auditors are permitted to provide advice or services other than audit to an audited entity, care should be taken that these services do not lead to a conflict of interest. In particular, auditors should ensure that such advice or services do not include management responsibilities or powers, which must remain firmly with the management of the audited entity.

23. Auditors should protect their independence and avoid any possible conflict of interest by refusing gifts or gratuities which could influence or be perceived as influencing their independence and integrity.

24. Auditors should avoid all relationships with managers and staff in the audited entity and other parties which may influence, compromise or threaten the ability of auditors to act and be seen to be acting independently.

25. Auditors should not use their official position for private purposes and should avoid relationships which involve the risk of corruption or which may raise doubts about their objectivity and independence.

26. Auditors should not use information received in the performance of their duties as a means of securing personal benefit for themselves or for others. Neither should they divulge information which would provide unfair or unreasonable advantage to other individuals or organisations, nor should they use such information as a means for harming others.

Chapter 4: Professional Secrecy

27. Auditors should not disclose information obtained in the auditing process to third parties, either orally or in writing, except for the purposes of meeting the SAI's statutory or other identified responsibilities as part of the SAI's normal procedures or in accordance with relevant laws.

Chapter 5: Competence

28. Auditors have a duty to conduct themselves in a professional manner at all times and to apply high professional standards in carrying out their work to enable them to perform their duties competently and with impartiality.

ISSAI 40: Quality Control for SAIs

A SAI should establish policies and procedures designed to provide it with reasonable assurance that the SAI, including all personnel and any parties contracted to carry out work for the SAI, comply with relevant ethical requirements.

- *SAIs should emphasise the importance of meeting relevant ethical requirements in carrying out their work.*
- *All SAI personnel and any parties contracted to carry out work for the SAI should demonstrate appropriate ethical behaviour.*
- *The Head of the SAI and senior personnel within the SAI should serve as an example of appropriate ethical behaviour.*
- *The relevant ethical requirements should include any requirements set out in the legal and regulatory framework governing the operations of the SAI.*
- *Ethical requirements for SAIs may include or draw on the INTOSAI code of ethics (ISSAI 30) and the IFAC ethical requirements, as appropriate to its mandate and circumstances and to the circumstances of their professional staff.*
- *SAIs should ensure policies and procedures are in place that reinforce the fundamental principles of professional ethics as defined in ISSAI 30, i.e.:*
  - *integrity;*
  - *independence, objectivity and impartiality;*
  - *professional secrecy; and*
  - *competence.*
- *SAIs should ensure that any parties contracted to carry out work for the SAI are subject to appropriate confidentiality agreements.*
- *SAIs should consider the use of written declarations from personnel to confirm compliance with the SAI's ethical requirements.*
- *SAIs should ensure policies and procedures are in place to notify the Head of the SAI in a timely manner of breaches of ethical requirements and enable the Head of the SAI to take appropriate action to resolve such matters.*
- *SAIs should ensure appropriate policies and procedures are in place to maintain independence of the head of the SAI, all personnel and any parties contracted to carry out work for the SAI.*
- *SAIs should ensure policies and procedures are in place that reinforce the importance of rotating key audit personnel, where relevant, to reduce the risk of familiarity with the organisation being audited. SAIs may also consider other measures to reduce the familiarity risk.*

ISSAI 200: General standards in government auditing and standards with ethical significance

2. Standards with ethical significance

2.1: The general auditing standards include:

(a) The auditor and the SAI must be independent.

(b) SAIs should avoid conflict of interest between the auditor and the entity under audit.

(c) The auditor and the SAI must possess the required competence.

(d) The auditor and the SAI must exercise due care and concern in complying with the INTOSAI auditing standards. This embraces due care in planning, specifying, gathering and evaluating evidence, and in reporting findings, conclusions and recommendations.

Independence

2.3 Whatever the form of government, the need for independence and objectivity in audit is vital. An adequate degree of independence from both the legislature and the executive branch of government is essential to the conduct of audit and to the credibility of its results

2.21 Conditions of tenure for the head of the SAI can contribute to the SAI's independence from the executive, for instance through appointment for a lengthy fixed term or until a specified retirement age. Conversely, tenure conditions which put an SAI under pressure to please the executive would have an erosive influence on independence. For this reason it is in principle desirable that provisions relating to the termination of appointment or removal from office should be exercisable only by special process akin to that relating to the holders of judicial or like office.
2.27 The SAI should not participate in the management or operations of an audited entity. Audit personnel should not become members of management committees and, if audit advice is to be given, it should be conveyed as audit advice or recommendation and acknowledged clearly as such.
2.28 Any SAI personnel having close affiliations with the management of an audited entity, such as social, kinship or other relationship conducive to a lessening of objectivity, should not be assigned to audit that entity.
2.29 Personnel of the SAI should not become involved in instructing personnel of an audited entity as to their duties. In those instances where the SAI decides to establish a resident office at the audited entity with the purpose of facilitating the ongoing review of its operations, programs and activities, SAI personnel should not engage in any decision making or approval process which is considered the auditee's management responsibility.
Conflict of interest
2.31 SAIs should avoid conflict of interest between the auditor and the entity under audit.
2.32 The SAI performs its role by carrying out audits of the accountable entities and reporting the results. To fulfil this role, the SAI needs to maintain its independence and objectivity. The application of appropriate general auditing standards assists the SAI to satisfy these requirements.
Competence
2.35 Discussion within the SAI promotes the objectivity and authority of opinions and decisions...
Due Care
2.40 The SAI must be, and be seen to be, objective in its audit of entities and public enterprises. It should be fair in its evaluations and in its reporting of the outcome of audits.
2.41 Performance and exercise of technical skill should be of a quality appropriate to the complexities of a particular audit. Auditors need to be alert for situations, control weaknesses, inadequacies in record keeping, errors and unusual transactions or results which could be indicative of fraud, improper or unlawful expenditure, unauthorised operations, waste, inefficiency or lack of probity.
2.46 Information about an audited entity acquired in the course of the auditor's work must not be used for purposes outside the scope of an audit and the formation of an opinion or in reporting in accordance with the auditor's responsibilities. It is essential that the SAI maintain confidentiality regarding audit matters and information arising from its audit task. However, the SAI must be entitled to report offences against the law to proper prosecuting authorities.

10. Integrity awareness

10.1 Description

As well as measures to increase the organisation's resilience to integrity violations, investments should be made in the moral resilience of individual members of staff. Integrity, or the integrity of an act, stands or falls on the integrity of the persons involved. Attention should therefore be paid to training and educating civil servants so that they can respond correctly in high-risk situations or if faced with dilemmas at work.

10.2 Key questions

- Is integrity an explicit requirement for all positions?
- Are regular training courses given to consider integrity?

- Are staff in vulnerable positions informed of particular risks and counter measures?
- Do staff get special assistance and/or council to cope with integrity risks?

10.3 Notes

Integrity as explicit requirement for all positions

If an organisation names integrity as one of its core requirements for its staff, moral competence will be systematically included in staff development.

Integrity training (dilemma training, moral judgment)

Investments must be made to strengthen the moral competence of the staff. Moral competence is the willingness and ability to carry out tasks adequately and carefully in the light of all applicable responsibilities, even in new, changing and complex situations for which there are no clear guidelines. Training courses teach civil servants how to arrive at the morally correct conclusion, one that is in keeping with the organisation's values and standards.

Inform staff of integrity risks and measures

Taking appropriate measures to reduce exposure to integrity violations is not enough. The organisation must also fully inform the staff in vulnerable positions about the integrity risks and the integrity measures in place. The staff must be made aware of the potential pitfalls and be receptive to early signs of misconduct and respond to them. If so, the organisation can make strict demands on the staff who carry out vulnerable activities. These members of staff should therefore be screened (see also the section on personnel management). The screening should also consider the staffs' personal circumstances and conduct, for example whether they are in debt, are addicted, etc.

Integrity assistance / council

The integrity counsellor (also) plays an advisory role. As well as being a contact point, the integrity counsellor is a source of advice for civil servants facing an integrity issue.

11. Management attitude

11.1 Description

Organisations and management styles differ from each other in many respects. The management style adopted by an organisation will influence its integrity. The management itself must set a good example and actively conduct an integrated integrity policy. If management sets the wrong example, the staff will be more inclined to copy its behaviour and will also be guilty of lack of integrity. If management does not implement an integrity policy, or does so only half-heartedly, it will give the impression that integrity does not enjoy high priority.

11.2 Key questions

- Does management actively promote the importance of integrity?
- Does management actively seek the implementation of an integrity policy and integrity measures?
- Does management always respond appropriately to integrity issues?
- Does management itself comply with integrity regulations and/or code of conduct, serving as an example of appropriate ethical behaviour (ISSAI 40, 6b, element 2)?

11.3 Notes

Management's promotion of the importance of integrity
It is not enough for managers to show that they themselves act with integrity. They must show in word and deed that integrity is important, that integrity calls for vigilance and that through the integrity policy the organisation helps the staff to be good civil servants. They can do so in word by emphasising the importance of integrity, for example in the organisation's mission statement, in speeches, in internal media and in informal contacts. They can do so in deed by developing and formally adopting an integrity policy, by providing people and resources for it and by ensuring that it is implemented.

Management steering
Management should actively seek the implementation of an integrity policy and integrity measures. In doing so, it should strike a balance between:
- preventive and repressive measures,
- compliance and encouragement.

An integrity system should contain both preventive and repressive components. Preventive components are designed to stop integrity violations whereas repressive components are designed to detect, investigate and punish violations. If an integrity violation goes unpunished, it will lead to a loss of motivation among the organisation's willing members of staff. Although both components are needed, the investment should concentrate on preventive measures. The effort that has to be taken to prevent incidents is more sustainable, is more positive, has a wider impact and is less than the effort that has to be taken to investigate and repair the damage and to restore confidence after an incident.

An integrity system should include elements of both compliance and encouragement. The compliance strategy is rule-based and, as such, is directed at the imposition of regulations, guidelines and procedures from above and controlling and punishing unacceptable behaviour. The encouragement strategy is directed at fostering awareness of and responsibility for integrity among staff (moral competence). As a rule of thumb, a good balance is compliance where necessary, encouragement where possible.

Dealing with integrity issues
Managers should deal with integrity issues carefully because the staff will take note of their response and follow their example. The correct management response will have a positive impact on the staff's integrity awareness. See also the notes in section 10.3 on the response to integrity violations

Exemplary role of management
A civil servant should act "as befits a good civil servant". In the first instance, a civil servant is responsible for his own acts and omissions. If the organisation and management are good employers, they will encourage and support their staff in this area. The management, from top to bottom, must set a good example for the staff and be beacons of integrity. They should be aware that their staff not only listen to what they say but, above all, watch what they do.

12. Organisational culture

12.1 Description
The organisational culture shapes the way in which the organisation's staff deal with each other (internal) and with third parties (external). Culture is a complex area and has a great

influence on integrity within the organisation. Organisational culture also includes less formal forms of conduct such as the working atmosphere, the leadership style, the ability to discuss issues and private problems, comradeship and loyalty, the organisation's openness to criticism and its tolerance of errors.

The attention management pays to integrity, the importance it attaches to it and whether there is open communication about it, the openness with external parties, the institutionalisation of integrity through consultation and performance interviews and the openness shown when dealing with integrity violations are also important aspects of the organisational culture. The key to promoting integrity through the organisational culture is communication. Management should encourage the discussion of problems and dilemmas and the provision of advice.

12.2 Key questions

- Is regular attention paid to the importance of integrity?
- Can integrity questions be discussed safely?
- Is there sufficient opportunity to express criticism?
- Is the importance of integrity clearly explained to external relations?
- Is there open communication on integrity violations and how they are dealt with?
- Is there a culture of holding others responsible for their conduct?
- Is there sufficient consideration of job satisfaction?

12.3 Notes

Internal openness and communication

Having an integrity policy is one thing. Communicating it is at least as important. To ensure that adequate and permanent attention is paid to the importance of integrity, the entire arsenal of available communication means must be deployed. If an organisation does not pay enough attention to integrity or highlight its importance, it opens the door to risks. On the one hand, it might lead to staff not realising how much importance the organisation attaches to integrity. On the other, it might lead to uncertainty about the conduct the organisation expects from the staff and what the staff must do from an integrity angle. It is therefore important that the organisation regularly raises the issue of integrity. By doing so, it will show that integrity is important and that staff are expected to act with integrity. Integrity can be communicated in various ways and at various times:

- during performance interviews and work consultation;
- by producing and disseminating information;
- through the organisation by supporting managers with information packs and targeted training so that they can approach integrity in a natural and professional manner;
- during internal courses and external training courses.

Ability to discuss problems, dilemmas and criticism with superiors and colleagues

The ability to discuss private and professional problems is an important condition for integrity. If they cannot be discussed, staff will not be able to find answers. There is a risk of the situation deteriorating and culminating in a loss of integrity. The same is true of concrete dilemmas that might arise at work. If they cannot be discussed, there is a risk of over-reliance on a member of staff's personal opinions and judgments. Managers in particular should be receptive to problems, dilemmas and criticism. But colleagues should also be able to address each other on their conduct. There is a culture of responsibility if colleagues do not think twice about discussing difficult issues or the substance and limits of their

responsibilities with each other, whether they have been asked to do so or not, in order to clarify and test common moral positions and to seek applicable moral frameworks.

External openness and communication
Good communication with third parties also contributes to an organisation's integrity. An organisation with an open culture states what it stands for and what it is responsible for. Such openness is particularly important in contacts with the public, suppliers, businesses and social institutions. Publishing codes of conduct on the internet or, even better, actively distributing them or involving external parties in their preparation contributes to a good understanding of each other's expectations and obligations.

Openness when dealing with integrity violations
An important aspect of an organisation's culture is its consistent response to integrity violations. Taking no action or responding half-heartedly is a signal to staff that the organisation does not value integrity. In consequence, one person's lack of integrity encourages another's. There is also the risk of initially minor infringements growing into more serious violations if left uncorrected. Regardless of an infringement's seriousness, management should act consistently and conscientiously and communicate the response to the staff and organisation so that it is clear that such conduct is not tolerated.

Holding each other responsible
An important aspect of an open culture that promotes integrity is that members of staff can hold each other responsible for their behaviour and so help maintain the organisation's integrity.

Job satisfaction
Lack of job satisfaction among the staff can have all manner of negative consequences for the organisation, such as low productivity and high absenteeism. It is also a fertile breeding ground for unacceptable conduct. Management should therefore be alert to signs that staff have little or no satisfaction in their work. Conditions of employment have a great impact on job satisfaction and thus the integrity of the staff. Salary, ability to take training courses and opportunity to progress within the organisation all contribute to job satisfaction. Badly-paid staff are susceptible to bribery. Staff who cannot progress further can become dissatisfied and bitter and thus represent an integrity risk. The organisation should therefore recognise the importance of the remuneration structure and the training and development plans in place for individual members of staff.

13. Recruitment & selection

13.1 Description
The staff are the organisation's social capital. That is why integrity policy should centre on the staff. Human Resource Management (HRM) and personnel policy provide many opportunities for the organisation to consider staff integrity.

13.2 Key questions
- Is a fixed procedure in place to deal with all applications?
- Is an advisory selection committee consulted?

- 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)?
- Are CVs, diplomas, references, etc. always checked?
- Is integrity part of the induction programme for new members of staff?
- Where necessary, do staff sign a declaration of confidentiality?
- Is integrity periodically considered in work consultation and performance interviews?
- Is integrity a specific consideration when hiring temporary and external staff? (ISSAI 40, 6b, element 2)
- Is integrity considered when staff leave or during exit interviews?

13.3 Notes

Recruitment, selection and hiring procedures

The organisation must guard against taking on "rotten apples", or dishonest staff, when employing new personnel. Experience shows that inappropriate behaviour by one person induces similar behaviour by others. Such a person represents a serious threat to the organisation's integrity. It is therefore important that the organisation has a good employment policy. The selection of new personnel should consider not only professional qualities such as education and work experience but also the trustworthiness of new members of staff. This in any event includes:

- the introduction and observance of a fixed application procedure to prevent arbitrary decisions and favouritism. A decision to employ someone should be taken by more than one person (e.g. by a selection committee);
- CVs, diplomas and references should be checked in order to gain an impression of the applicant's background and his performance (and integrity) in previous positions.

Screening

ISSAI standards (ISSAI 1: Lima declaration; Section 14.1) require members and staff of SAIs to be evaluated on qualifications and moral integrity in order to ensure that they can fully carry out their tasks.

Staff should be screened not only when they join the organisation but also when they change positions. The screening should be periodically repeated and may include:

- a check of the applicant's record;
- the submission of a certificate of good behaviour;
- a security check (intelligence and security services).

Consideration of integrity during introduction

New members of staff do not know the regulations, procedures and conduct expected by the organisation they have just joined or the channels they should use to raise integrity issues. Some time is needed for a new member of staff to find his feet. In the beginning, both he and the organisation will be vulnerable. New members of staff should therefore be informed about the importance of integrity when they join the organisation. This is where a good introduction policy with specific consideration of integrity can help. A good introduction policy includes:

- taking an integrity-related official oath or pledge;
- explaining and providing the code of conduct;
- introducing the integrity counsellor.

Declaration of confidentiality
New members of staff should be informed of any integrity issues in their work. Having them sign a declaration of confidentiality is a special means to bring such issues to their attention.

Consideration of integrity during work consultation and performance interviews
The subject of integrity should be raised at various moments. Since integrity policy should be a fixed part of personnel policy, integrity should also be considered during work consultation and performance interviews.

Hiring temporary or external personnel
External staff are often taken on to overcome temporary capacity problems or to provide specific expertise that the organisation itself does not have. Extra care should be taken with such staff since they will not be aware of the specific rules and procedures (structure) or values (culture) prevailing in the organisation. The organisation should be prepared for this and formulate a specific policy for external personnel.

Consideration of integrity when staff leave
Employees may leave the organisation for a variety of reasons. They might retire, a temporary contract might end, they might find another job because they seek different work or are dissatisfied with the organisation. Whatever the reason, exit interviews should always be held when a member of staff leaves. The employer should know why people leave the organisation. People can be unhappy with the culture, their salaries, the management or the career prospects. This is important input for the organisation because these factors might kindle unacceptable conduct. When staff leave the organisation they feel freer to talk about such things and will voice their opinions more readily. They might also point out where the organisation can make improvements. As part of the exit policy:

- exit interviews should be held whenever a member of staff leaves;
- during the exit interview, the employee should be asked where improvements can be made;
- the question of integrity should be raised during the exit interview;
- a report should be made of all exit interviews;
- exit interviews should be recorded and coordinated by the personnel department;
- annual analyses should be made of the reasons for leaving and the points for improvement.

14. Response to integrity violations

14.1 Description
As well as preventive measures to stop integrity violations occurring, the organisation should be fully prepared for an integrity violation or the suspicion of one. An effective response to a violation (whether real or suspected) will also help prevent future violations. It confirms the values and standards and encourages staff to resist temptation. Suspicion of a violation quickly leads to unrest and tension within the organisation. Good preparation can prevent further escalation and help restore calm. Essential measures include:

- notification and complaints procedures to identify actual or potential violations in good time;
- systematic investigation procedures;
- sanctions (punishment) set in a clear framework;

- records of actual or potential violations and punishments.

14.2 Key questions
- Is a notification procedure in place for employees to report suspected violations ('whistle blowers procedure)? (ISSAI 40, 6b, element 2)
- Are managers accessible by employees to report suspected violations?
- Is an integrity counsellor involved in the notification of violations?
- Is there a procedure for handling signals and complaints from external sources?
- Is there a protocol to investigate integrity violations?
- Are integrity violations recorded centrally?
- Does the organisation always respond to integrity violations?
- Are suspicions of criminal offences reported to the public prosecutor or the police?
- Are incidents evaluated and discussed with staff involved?

14.3 Notes
Notification procedure and involvement of management and integrity counsellors
Before it can respond to an integrity violation, the organisation's management must know about it. Procedures must therefore be in place to report misconduct and to protect civil servants who bring such misconduct to management's attention. Such procedures are commonly known as whistleblower schemes. They usually describe kind of misconduct that must be reported, such as:
- serious offences;
- gross violations of regulations or rules;
- the deception of judicial authorities;
- serious threats to public health, safety or the environment;
- deliberate suppression of information on such misconduct.

A precondition for reporting is that management should be accessible by employees to report suspected violations.

Notifications must be based on "reasonable suspicions" and must not be made with a view to personal gain or to criticise policy decisions. The notification procedure must complement the design of the counsellor's function in the organisation. As well as a notification procedure, a complaints procedure helps receive external signals about possible misconduct (for example from members of the public).

Handling signals and complaints from external sources
The organisation should not only have procedures in place for internal whistle blowers, but also for handling signals and complaints from external sources.

Investigation protocol
A protocol or procedure should be in place to investigate reports of potential misconduct. It should lay down, for example, how the investigation will be carried out and who will be responsible for it.

Record misconduct
The records should contain, amongst other things, the notification of actual or potential violations, information on the follow-up to notifications and the sanctions applied. The records form the basis for the information supplied to management.

Sanctioning (response to violations)
The sanctioning (punishment) of integrity violations should be based on a sanctions policy that sets out the criteria that are used to decide how an integrity violation will be punished. The sanctions policy shows the personnel how seriously management take integrity. In this light, a record should be kept of sanctions imposed in the past and the reasons for doing so.

Reporting to the public prosecutor or the police
If it is thought that a criminal offence has taken place, it can be reported to the public prosecutor or the police. In some cases, it might even be obligatory to report such incidents. Disciplinary measures might also be imposed, such as reprimands, suspensions, transfers or (dishonourable) dismissals.

Evaluation of incidents
To learn from incidents it is important to evaluate integrity violations after they have been investigated. Perhaps the violation is not an incident and points at a broader pattern of integrity breaches. It is also useful to find out whether (systematic) weaknesses in the controls have made the violation possible. Finally integrity violations and their consequences may have a significant impact on staff working in the environment where the violation took place, for example direct colleagues of the offender.

15. Accountability and transparency

15.1 Description
An organisation's integrity is of great importance to both its internal and external stakeholders. Management should therefore account both internally and externally for the design and operation of the integrity control system and any changes in it. Accountability also makes management feel more responsible for their organisation's integrity.
ISSAI 20 devotes special attention to accountability and transparency as an element of good governance of the SAI. This is explicitly reflected in the key questions of this cluster of the integrity control system.

15.2 Key questions
General
- Does senior management receive reports to account for the integrity policy conducted?
- Do staff representatives receive reports to account for the integrity policy conducted?
- Do democratically elected authorities (parliament, municipal council, etc.) receive reports to account for the integrity policy conducted?
- Are the reports systematically structured and containing clear indicators?

Specific for SAIs
- Are the SAI's mandate, role, responsibilities, organization, mission, strategies, audit manuals, procedures and criteria public (ISSAI 20, chapter 2/3)?
- Are the SAI's audit findings and conclusions subject to contradictory procedures (consultation with the audited entity) (ISSAI 20, chapter 3)?
- Are the SAIs accounts public and subject to external audit or parliamentary review (ISSAI 20, chapter 4)?
- 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)?

- Are the status of auditors (magistrates in the Court model, civil servants or others), their powers and obligations public (ISSAI 20, chapter 5)?
- 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)?
- Are codes of ethics issued and public (ISSAI 20, chapter 5)?
- 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)?

15.3 Notes
Internal accountability (management and staff representatives)
Periodic integrity reports should be submitted to the senior management and the staff representatives. The account rendered to senior management could form part of the organisation's planning and control cycle. The report to the staff representatives could be provided in the Social Annual Report or a similar document.

External accountability (democratically elected authorities)
The organisation should also account externally for its integrity, for example in the form of an annual report, to democratically elected authorities such as parliament or municipal council. By doing so, it acknowledges the importance of integrity to the organisation's external stakeholders.

An account should also be rendered to the organisation's supervisors as well as to the democratically elected authorities. Supervisors can then form a picture of the integrity control system they supervise and determine whether there are any weaknesses.

Within the public sector there is a general duty of accountability to the public. The public involuntarily contribute the public funds without which the public sector would be unable to function. The exclusive nature of public tasks (such as the power to take coercive measures) also means that the public must be given assurances that integrity is safeguarded wherever possible. By means of an external account, for example in an annual report or through another public channel such as the internet, interested members of the public can gain an insight into the design and operation of integrity management.

Systematic reporting structure and clear indicators
The value of reports to account for integrity policies increases when a systematic reporting structure is used and clear indicators are included in the reports.

SAI standards
Due to the typical nature of SAIs high standards apply for transparency and accountability. This is reflected in the standards mentioned in ISSAI 20: "Principles of Transparency and Accountability".

16. Audit and monitoring

16.1 Description
Integrity audits are a fitting means for management to gain an insight into the quality of the organisation's integrity control system. Such audits can be carried out by an internal control /

audit department or by an external auditor. They are more valuable if management is aware of the integrity audit findings and recommendations and consistently responds to them.

16.2 Key questions

- Is the integrity system periodically audited by an internal auditor?
- Is the integrity system periodically reviewed by an external auditor and/or supervisor?
- Is the integrity system periodically monitored or evaluated by management?

16.3 Notes

Internal (internal control/audit department)

The internal control or audit department should carry out integrity audits and report its findings to the organisation's management. Before the audit starts, decisions must be taken on its scope and depth. This provides an opportunity to meet management needs in so far as possible. However, it might also have an adverse impact on the audit's independence.

External (external auditor/supervisor)

The external auditor and/or supervisor reviews and reports on the organisation's integrity management. In the case of external audit, the auditor or supervisor will determine the audit scope and depth (with reference to appropriate legislation). This improves the audit's independence. For an external audit to have a positive impact, however, it must produce results that management can use.

Monitoring and policy evaluation

Integrity policy must be expressed in concrete goals and activities. To prevent the goals and activities from being overlooked, they should form part of the planning & control cycle set up to monitor the organisation's processes. Within this structure, management reports inform the senior managers of the implementation of the agreed activities and their outcome. Periodic checks should be made of the policy achievements. Were the agreed activities and measures implemented and did policy have the desired outcome? If the outcome is not entirely satisfactory, policy should be revised.

8.4 Maturity level assessment

The maturity level assessment of the integrity control system 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.

It would be too complex to include all these elements separately in the assessment method. Therefore a relatively simple method has been designed for scoring the maturity level:

Level	Criteria
0	- The measure does not exist
1	- The measure exists - The measure is not implemented / not observed
2	- The measure exists - The measure is implemented / observed - The measure is not effective
3	- The measure exists - The measure is implemented / observed - The measure is effective

The score indicates the maturity level already achieved. In principle, the maturity level required is the highest level. In certain organisations, however, some measures will be less relevant or not applicable. This will become clear when the maturity level is scored and discussed by the participants.

The assessment of the maturity level considers all the relevant measures and their effect. If the assessment method is applied to a department of a larger organisation, the measures applicable to the organisation as a whole are also considered as well as those in place specifically for the department.

Scoring the maturity level of the integrity control system
To score the maturity level of the integrity control system it is easiest to have group members award their scores individually or in small groups. If necessary individual scores can be discussed and eventually be adjusted.

The group score for the maturity of the Integrity Control System is reached in 3 steps:
1. assessing the maturity level of each measure by averaging individual scores and group discussion ;
2. defining the maturity level of each cluster by computing the average of the measures in the cluster;
3. defining the maturity level of the entire Integrity Control System by computing the average of the clusters.

8.5 Analysing strengths and weaknesses of the integrity control system

Based on the complete assessment of the Integrity Control System it is now possible to summarise the results on the main clusters. This will enable an analysis of the relative strengths and weaknesses of the system, by entering the average scores of the maturity level for each cluster and then calculate the total average score (see the table below). The scores are entered in the management report.

Nr.	Clusters of controls	Average	Level
	General controls		
1	Policy framework		
2	Vulnerability / risk analysis		
13	Recruitment and selection		
14	Response to integrity violations		

15	Accountability		
16	Audit and monitoring		
	Hard controls		
3	Responsibilities		
4	SAI legal framework		
5	Integrity legislation and regulations		
6	Administrative organisation and internal control		
7	Security		
	Soft controls		
8	Values and standards		
9	Professional SAI standards		
10	Integrity awareness		
11	Management attitude		
12	Organisational culture		
	Overall average score of all clusters		

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 maturity level is input for the gap analysis in Chapter 9.

9 Gap analysis and recommendations

9.1 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 (for example both on a medium level) it may still be desirable to reduce some of the identified vulnerabilities or to address specific controls that need strengthening.

The IntoSAINT gap analysis focusses on the level of the entire organisation or the object as defined in the first phase of the methodology, if the assessment does not encompass the entire SAI. On this level of aggregation the participants consider the identified vulnerabilities and the maturity level of the integrity controls. In addition to the workshop it is possible to conduct a gap analysis on the more detailed level of specific risks, but this option is not covered in this manual.[7]

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.

Another possibility to reduce vulnerability is to address vulnerability enhancing factors. Sometimes this can be done by organisational change or redesigning procedures, for instance, to reduce unnecessary complexity.

A complementary 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.

Balance between vulnerabilities and controls

First we need to establish whether the maturity of the organisation's integrity control system balances the organisation's vulnerability profile. For this we compare the total vulnerability score with the total maturity level score. The (im)balance is established at an aggregate level, meaning that the gap analysis on this level is not intended to assess whether there is an exact link between a specific vulnerability and a specific control measure. As shown in chapter 8 the integrity control system also includes general (clusters of) controls that are not specifically designed to address one specific vulnerability or risk, but aim for a broader impact on the resilience against integrity violations. Examples are formulating an integrity

[7] Specific guidance for a detailed risk assessment is separately available.

policy and integrity awareness training. So the gap analysis on this level will help to establish whether the entity's overall resilience is consistent with its overall level of vulnerability.

In plenary sessions the workshop participants will discuss the most relevant vulnerabilities identified during the assessment, the most striking weaknesses in the integrity control system, as well as the possible links between the two. The objective of this discussion is to arrive at a shared picture of the organisation's main vulnerabilities and what causes them and management recommendations on how to reduce vulnerabilities and/or to improve the integrity control system.

Reducing vulnerabilities and strengthening controls

During the next session of the workshop the participants will work in subgroups. One or two subgroups may focus in more detail on the specific scores on inherent vulnerabilities and vulnerability enhancing factors. These subgroups are asked to consider possibilities to reduce the level of vulnerability, especially in case the vulnerability scores are relatively high. The other subgroups will revisit the maturity scores cluster by cluster and discuss specifically the integrity controls with relatively low scores. These subgroups should consider opportunities for strengthening controls.

This part of the gap analysis provides the basis for formulating recommendations to management, which is the next step in the methodology.

9.2 Recommendations and reporting

A thorough gap-analysis leads to well based recommendations on how to reduce the general risk level by setting priorities and implementing new measures or improving existing measures.

In this part of the workshop the following questions are answered:

- What should be improved?
- What should management do?

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.

To collect recommendations the participants will work in the same subgroups identified during the gap analysis (see 9.1). The subgroups write recommendations either to reduce vulnerability or to strengthen controls on post-its. During the following plenary session the moderators will help the participants to combine and cluster the recommendations in relevant topics and to score them on priority and importance. It is important to add a timeline indicating how soon the implementation of the recommendations could start.
At the end of this session the moderators will summarise the recommendations and management priorities again and reconcile this with the participants to make sure that the summary reflects the opinion of the group.
On this basis the moderator(s), in cooperation with the workshop coordinator, prepare a draft report and a management presentation.[8]

[8] Templates for both are part of the workshop material.

Finally the assessment report, including the recommendations, should be presented to management, since management is primarily responsible for the adequacy of the integrity control system. Preferably a delegation of the participants should attend the meeting in which the workshop results are presented to management, since it reflects their assessment and the participants may answer questions from management and provide comments.

To stimulate awareness and support for the integrity approach in general and for specific measures, it is recommendable to communicate the results of the workshop extensively across the organisation.

Annex: 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		**SAI legal framework**
	4.1	Existence and independence of the SAI embedded in the Constitution (ISSAI 10; principle 1)
		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)
	4.3	- a sufficiently broad mandate and full discretion, in the discharge of SAI functions (ISSAI 10, principle 3)
	4.4	- unrestricted access to information (ISSAI 10, principle 4)
	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)
	4.6	- financial and managerial / administrative autonomy and the availability of appropriate human, material and monetary resources (ISSAI 10, principle 8)
5		**Integrity legislation and regulations**; Rules are in place regarding:
		Conflicts of interest
	5.1	- external positions/financial interests
	5.2	- the acceptance of gifts/invitations
	5.3	- confidentiality
	5.4	- preventing “revolving door arrangements”
	5.5	- external screening of contractors and/or licence applicants
	5.6	- lobbying
	5.7	- influence of politicians on civil servants
		Integrity within organisations
	5.8	- combating/dealing with undesirable conduct
	5.9	- expense claims
	5.10	- email, internet and telephone use
	5.11	- use of the employer’s property
6		**Administrative organisation and internal control**
	6.1	Specification of vulnerable activities and positions
	6.2	Specific procedures in place for conducting vulnerable activities
	6.3	Job descriptions for all staff members
	6.4	Segregation of duties
	6.5	“Four eyes principle” applied
	6.6	Mandate regulations

Cluster	Measure	
	6.7	Job rotation scheme (ISSAI 40, 6b, element 2)
7		**Security**; Measures have been taken with regard to:
	7.1	physical security (locks, windows, doors, safes, etc.)
	7.2	Information security (IT security, clean desk policy, classification of information as confidential/secret, access authorisations, filing systems)
8		**Values and standards**
	8.1	Integrity is part of the organisation's mission
	8.2	Core values have been formulated (e.g. impartiality, professionalism etc.)
	8.3	(Integrity) code of conduct
	8.4	Oath or pledge
	8.5	Special ceremony for taking the oath or pledge
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)
	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)
	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)
	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)
	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)
	9.6	Employees have been involved in the formulation of the code of ethics and/or the standards with ethical significance
10		**Integrity awareness**
	10.1	Integrity is an explicit requirement for all positions
	10.2	Regular training courses considering integrity
	10.3	Staff in vulnerable positions informed of particular risks and counter measures
	10.4	Special assistance and/or council for staff to cope with integrity risks
11		**Management attitude**
	11.1	Management actively promotes the importance of integrity
	11.2	Management actively seeks the implementation of an integrity policy and integrity measures
	11.3	Management always responds appropriately to integrity issues
	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)
12		**Organisational culture**
	12.1	Regular attention is paid to the importance of integrity
	12.2	Integrity questions can be discussed safely
	12.3	Sufficient opportunity to express criticism
	12.4	Importance of integrity is clearly explained to external relations
	12.5	Open communication on integrity violations and how they are dealt with
	12.6	Culture of holding others responsible for their conduct
	12.7	Sufficient consideration of job satisfaction

Cluster	Measure	
13		**Recruitment & selection**
	13.1	Fixed procedures for dealing with all applications
	12.2	Advisory selection committee
	13.3	Checking of CVs, diplomas, references, etc.
	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)
	13.5	Integrity is part of the introduction programme for new members of staff
	13.6	Declaration of confidentiality signed by staff
	13.7	Integrity is periodically considered in work consultation meetings and performance interviews
	13.8	Integrity is a specific consideration when hiring temporary and external staff (ISSAI 40, 6b, element 2)
	13.9	Integrity is considered when staff leave or during exit interviews
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)
	14.2	Managers are accessible by employees to report suspected violations
	14.3	Integrity counsellor is involved in the notification of violations
	14.4	Procedure for handling signals and complaints from external sources
	14.5	Protocol for investigating (suspected) integrity violations
	14.6	Central recording of integrity violations
	14.7	The organisation always responds to integrity violations
	14.8	Suspicions of criminal offences are always reported to the public prosecutor or the police
	14.9	Incidents are evaluated and discussed with staff involved
15		**Accountability**
		General
	15.1	Senior management receives reports to account for the integrity policy conducted
	15.2	Staff representatives receive reports to account for the integrity policy conducted
	15.3	Democratically elected authorities (parliament, municipal council, etc.) receive reports to account for the integrity policy conducted
	15.4	Reports are systematically structured and containing clear indicators
		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)
	15.6	The SAI's audit findings and conclusions are subject to contradictory procedures (consultation with the audited entity) (ISSAI 20, chapter 3)
	15.7	The SAIs accounts are public and subject to external audit or parliamentary review (ISSAI 20, chapter 4)
	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)
	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)
	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)
	15.11	Codes of ethics are issued and public (ISSAI 20, chapter 5)
	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)
16		**Audit & monitoring**
	16.1	The integrity system is periodically audited by an internal auditor
	16.2	The integrity system is periodically reviewed by an external auditor and/or supervisor
	16.3	The integrity system is periodically monitored or evaluated by management