Integrity Assessment of Public Sector Organisations

MANUAL

Integrity Vulnerability mapping

2014

Contents

Introduction

This manual describes a methodology for the assessment of integrity vulnerability and corruption risks in public sector organisations. The assessment method focuses on the prevention of corruption as a very important issue for the integrity of the public sector. It is the first part of an integrated integrity assessment approach, of which the second and complementary part deals with the assessment of the maturity of integrity controls.

This assessment methodology is general in its nature and may be part of an audit approach. Also this assessment may be part of integrated or comprehensive audits. Another way of using the method is within the framework of a (controlled) self assessment.[1]

This manual consists of two parts:

Part I	Principles of the methodology
Part II	Guidance for application

[1] An example is SAINT (Self Assessment INTegrity). This is a tool developed by the NCA on which parts of this methodology are based.

Part I: Principles of the methodology

1 Integrity and audit

1.1 The role of the Supreme Audit Institution (SAI)

Building, maintaining and strengthening public institutions, the fundament of a constitutional state, is considered a key to controlling corruption.[2]

Among public institutions, the SAI can play a critical role, as they help promote sound financial management and thus accountable and transparent government. The full potential of SAIs to address corruption can be exploited when the role for SAIs in addressing corruption is not limited to detection and reporting about corruption 'after-the-fact'. SAIs can play an important role in preventing corruption and fraud, offering 'before-the-fact' advice and warnings.

The most common way to do that is by making use of 'early warning' signals that reviews of internal controls deliver. Auditors report to public sector organisations on the weaknesses in their internal controls.[3] These are the same weaknesses that can lead to corruption and fraud if not addressed. Why wait until after the fact? By engaging with risk assessments and audits early and actively, SAIs can address weaknesses in internal controls long before a fraud investigation or corruption commission comes into the picture. The 'under the surface' work done by audit's assessment and testing of internal controls aiming at preventing integrity breaches, fraud and corrupting can make a significant difference to the risk and cost of fraud and corruption in the public sector. [4]

SAIs are well situated to contribute; they are widely viewed as the independent watchdogs of the public interest. In some countries they are already putting a greater focus on accountability for "ethics in the public service" in the scoping of their audit work.

With this manual we offer guidance for an **integrity approach** in audit; an approach that contributes to strengthening the internal controls of public sector organisations towards integrity breaches and that promotes integrity awareness.

1.2 Role of the SAI auditor

Although the scope of audit within each SAI depends on regulations, mandate and organizational structure, we are convinced that the SAI and its auditors can integrate the integrity approach in some form in their daily audit work.

According to ISSAI 100[5] the full scope of government auditing includes regularity and performance audit.

---

[2] http://info.worldbank.org/etools/docs/library/18120/pillars.pdf (Date of consultation 12-3-2014)

[3] Control weaknesses like: poor security of internal information systems, lack of separation of duties in finance and banking, poor internal compliance monitoring of key policies and procedures, lax leave-management and inadequate record keeping for important decisions

[4] http://www.audit.vic.gov.au/presentations/APSACC-15-November-2011.pdf (Date of consultation 12-3-2014)

[5] ISSAI 100- "INTOSAI Auditing Standards- Basic Principles", paragraphs 38 and 39

Regularity audit embraces:

a) Attestation of financial accountability of accountable entities, involving examination and evaluation of financial records and expression of opinions on financial statements;
b) Attestation of financial accountability of the government administration as a whole;
c) Audit of financial systems and transactions including an evaluation of compliance with applicable statutes and regulations;
d) Audit of internal control and internal audit functions;
e) Audit of the probity and propriety of administrative decisions taken within the audited entity;
f) Reporting of any other matters arising from or relating to the audit that the Supreme Audit Institutions considers should be disclosed.

The integrity approach explained in this manual is directed at assessing the quality of the internal controls of the public sector institution, specifically at the internal controls that safeguard the integrity of the operations of the entity: elements d) and f).

The manual assumes that the auditor is familiar with the basic principles as mentioned in ISSAI 100. For the integrity approach the most relevant principles are:

- Auditors should obtain an understanding of the nature of the entity/programme to be audited
- Auditors should conduct a risk assessment or problem analysis and revise this as necessary in response to the audit findings

The first parts of this manual provides guidance on integrity risk assessment that helps the auditor to accommodate these principles.

2 Introducing the concept of integrity in public sector organisations

Traditionally the first resort in the fight against corruption is repression: a rule based approach that is focused on legislation, detection and prosecution of fraud and corruption. Although this approach is indispensable, there is more and more recognition of the fact that such a single handed approach is not enough, and can sometimes even be counterproductive. Enhancing the integrity of public sector organisations can offer a powerful complementary approach. It draws the attention to alternative values of ethics and integrity to replace a habit of corruption, thus opening up possibilities to replace unwanted behaviour of corruption by proposing desirable behaviour of integrity. This strategy is preventive, principle based and empowers the management and employees of public sector organisations in the fight against corruption.

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 is closely related to the absence of fraud and corruption, but it also entails common decency. In this way it is a positive and broad concept, that is related to ethics and culture. In this manual we use this wide and positive definition of the term integrity.

2.1 Responsibility for integrity in public sector organisations

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, social awareness, neutrality, considering all perspectives, 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.

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.

Organisations and its employees do not work in isolation. Cultural values, personal values, religious values etc. also influence what is considered to be ethical in a certain context. Although we recognise its importance it exceeds the scope of this manual.

2.2 Integrity: 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.

2.3 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 that may lead to dilemmas 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.

2.4 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".

2.5 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 integrity violations	Focus on facilitating good behaviour
Legal focus	Managerial focus
Repression/Reactive	Prevention/Pro-active

A well-balanced mix of both approaches is necessary for a sustainable result.

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.

3 Risk Assessment

Every public sector organisation faces a variety of risks from external and internal sources that may be assessed. Incidents of fraud, corruption and other integrity breaches damage the trust of the public in public sector organisations and prevent the public sector organisation to reach its objectives. It is the first responsibility of the management of public sector organisations to assess and control these risks. Proactive auditing seeks to establish to what extent the entity has established a process to detect, investigate and resolve integrity incidents.

Identification of risk of fraud and corruption is part of the over-all risk assessment a SAI normally undertakes while making the audit planning (ISSAI 100). This manual takes this principle one step further by giving a SAI specific guidance how to assess and monitor integrity risks for public sector organisations.

3.1 Risk analysis

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. 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.

Example: breaking and entering of your home:
According to what you know of the valuables in your house, incidents of burglary in the neighbourhood, quality of public lighting and police surveillance you will decide on: closing windows, locking doors, insurance, install bars, keep a dog or install an alarm-system.

Such exercises of risk analysis 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.

3.2 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.

Example: food security:

An undesirable event is have poisoned baby-milk sold in shops. This may not only cause illness or even death of babies and young children, but also damage the trust in the food industry, trust in the food security inspection, the government and the economy. So the impact is high. The probability depends on the quality of oversight and the (ethical) values of the companies involved. In The Netherlands the probability would be low, in China high.

3.3 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.

Example: local government:

An undesirable event is that a mayor riggs a bidding for a building contract to favour a friendly contractor, in exchange for an extention to his home. This may lead to a higher price for the contract, court cases by other contractors, or lower quality of the building. More dangerously this may lead to a culture of permissiveness and impunity if the ‘example’ set by the mayor goes without correction. Eventually this leads to loss of trust in the government, so the impact may vary. The opportunity is undeniable, but the probability depends on quality of the procurement procedure and control measures.

4 Vulnerabilities and temptations

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 is 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.

4.1 Vulnerabilities

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.

4.2 Temptations

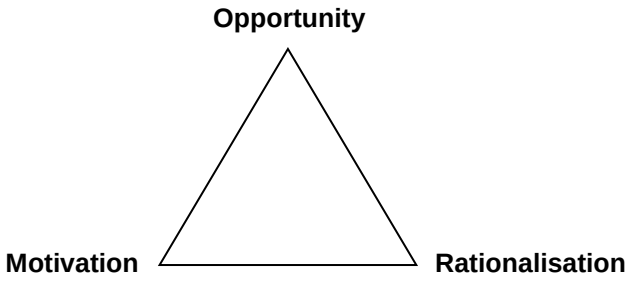
Most civil servants who commit an integrity violation did not intend to do so when they first entered the service. Many succumb to the temptations they face within the organisation. The temptations might be tangible (money, privilege) or intangible (status, recognition, protection). There are also "reverse 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.

4.3 Connecting vulnerabilities and temptations: Fraud triangle

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

When people commit fraud or corruption, there are three key elements which normally are present: 1. Motivation (Incentive/pressure); 2. Opportunity; 3. Rationalization. Together, these three elements constitute the so-called 'fraud triangle'. The fraud triangle is a simple, but powerful tool for auditors when assessing an entity’s vulnerability of fraud and corruption.



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.

Example: petty cash

If you are the keeper of the petty cash of your division, there is ample opportunity to ‘borrow’ some of its content for your personal use. If you are desperately short of money, you also have a motivation. Rationalisation may come from a lack of appreciation of your colleagues for the extra work that you do as keeper of the petty cash.

IThe methodology in this manual will consider the opportunities within the organisation that may lead to temptations (inherent vulnerabilities). Also the conditions for possible motivation and justification (rationalisation) which may lower the threshold for integrity violations (vulnerability enhancing factors) will be taken into account.

5 Basic aspects of the methodology

The methodology described in this manual is focussed on the assessment of:

- Inherent integrity vulnerabilities
- Vulnerability enhancing factors
- Vulnerability profile
- Major integrity risks
- Required control measures

5.1 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 with a view to preventing future violations.

5.2 Focus on public sector institutions

The assessment takes a public sector institution as its object. It is the managements responsibility to assure the organisation's integrity and have a sound integrity policy in place. Integrity must be a standard component in the management and policy cycle.

5.3 Thinking in terms of vulnerability and risk

The assessment method focuses on thinking in terms of vulnerability and risk. The result of the application of this methodology is a riks map. Based on this risk map it becomes clear what specific measures or controls need to be in place to mitigate these risks. Thinking in terms of vulnerability and risk is a specific skill that has to be learnt to formulate required integrity controls.

Part II: Guidance for application

6 Outline of the risk assessment method

The assessment methodology consists of four separate steps:

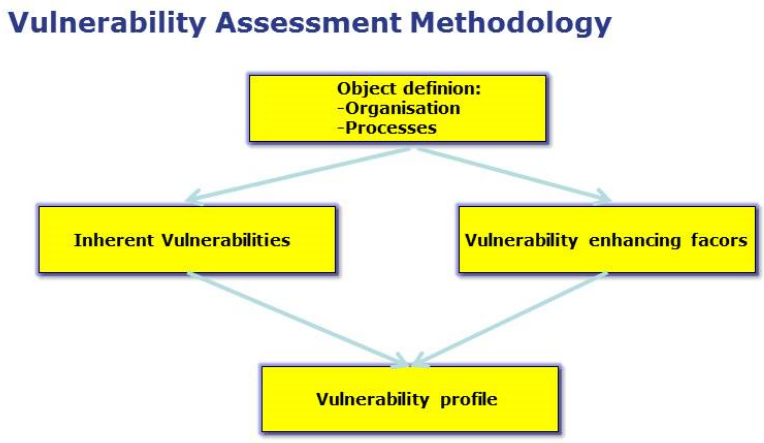
(1) Analysis of object and its processes
The first step is to define the object of the assessment and the relevant objectives and operations of the object that relate to the main tasks/processes. The object may be the entire organisation or specific organisational entities. For the selected object a description of its main tasks/processes has to be made.

(2) Assessment of inherent vulnerabilities
In this step, an estimate is made of the *vulnerability*, i.e. the potential exposure to integrity violations, of the organisation that performs the processes named in step (a). In this step the descriptions of tasks/processes is related to an overview of processes in the public sector that are known to be vulnerable to breaches of integrity.

(3) Assessment of vulnerability enhancing factors
This step will consider the presence or absence of vulnerability enhancing factors. These are circumstances within or around an organisation that raise the probability of an integrity violation occurring. In this step the knowledge of the auditor of the organisation is related to a list of these 'red flags'.

(4) Vulnerability profile
This step will produce an overview and overall assessment profile of the perceived vulnerability. Also it will indicate the most vulnerable processes and the top three integrity risks for the organisation.

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



6.1 Analysis of object and processes

The object of the assessment can vary. The object can be the public sector on a general level, specific parts of the public sector (e.g. clustered by themes or responsibility), semi-public institutions, specific processes and so on. The object of the assessment should be well-defined and clearly linked to management responsibility within the public sector organisations. To decide on the scope of the assessment is part of the strategic planning of the SAI.

In this manual the assumption is that the auditor will assess a specific organisation. When assessing more organisations, the manual promotes a systematic way of assessing and this will ensure that the assessments can be compared.

The following questions are essential:

1. Wat is the nature of the entity?
2. What organisational objectives and operations are vital?
3. What are the main tasks/processes performed by the (relevant part of the) organisation?

Given the scope of the assessment, what do you know of the public sector organization to be assessed. What is the amount of knowledge that the SAI possesses at the outset. The emphasis should always be on building a good understanding of the topic under examination in the shortest possible time. This might involve a single brainstorming session where a great deal of information is already known, or a larger data gathering exercise where the topic is new or complex.

Then start with reviewing what organisation objectives and operations are vital for the object. This has to be described in one-three sentences

The next step is to decide on the main tasks/processes. Most organisations have only a limited number of main tasks/ processes. To identify these main tasks/processes, the relevance for the organisation and their use of resources have to be considered. Usually the main tasks/processes can be retrieved from strategic documents of the object. They are often related to the (legal) duties of the organisation. It can help to also turn to the organizational structure. The tasks/processes in the description should be formulated in such a way that they are unambiguous. Usually this is described with verbs. It is recommended to avoid too much detail.

There are main tasks/processes specific to the type of organisation (primary processes): educating students and taking exams (for a school) or tax collection and the processing of financial information (tax administration). Consider tasks/processes defined as “a method to convert resources” (money, people, information, etc.) into products and services that achieve the organisation’s tasks and goals.
Other main tasks/processes can be more general/supportive, for example:

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.
5. Management support
   a) planning and control; the design and implementation of the planning cycle at strategic, tactical and operational levels;
   b) communication internal and with external parties
   c) internal control
   d) quality assurance

The conclusions of this step will be documented in a form 1: see Annexes.

Keep notes of the discussions and ideas so that you keep track of the background of the conclusions to add to the audit file.

6.2 Assessment of inherent vulnerabilities

From research, professional knowledge and experience it is known that some areas of activity in the public sector produce more integrity risks than others. For instance procurement or granting of subsidies are more vulnerable to breaches of integrity than teaching or archiving. 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 (cf Chapter 4). These are inherently vulnerable processes or functions.

Processes that have one or more of these characteristics are vulnerable to integrity violations. They 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, because they can provide a powerful motivation. This includes not only money, goods or real estate, but also information as a valuable public asset.

Inherent vulnerable processes or areas that are considered in this methodology are the following:

<u>Contracting</u>
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.

<u>Payment</u>
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.

<u>Granting / Issuance</u>
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.

<u>Regulating</u>

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. Suppliers of goods have an interest in acquiring profitable government contracts, which creates a vulnerability (see also contracting). Managing valuable goods is also 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.

These vulnerable processes or activities 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	purchasing / selling, management and consumption (stocks, computers)
	Real estate	buying / selling

To assess the level of inherent vulnerability the list of organisational processes is matched with the list of inherently vulnerable areas and check which vulnerabilities are present. The extent of vulnerability is indicated using the following scoring method.

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

The result is entered into form 2, see Annexes.

Keep notes of the discussions and ideas so that you keep track of the background of the scoring to add to the audit file.

6.3 Assessment of 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.).

The factors that are taken into account in this methodology are based on secondary analysis by the Netherlands Court of Audit of several cases of fraud and corruption both in the Netherlands and worldwide. Also what is commonly known in fraud literature as 'red flags' are included.

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

It must be stressed that presence of one or more of the vulnerability enhancing 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.

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
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
Personal threats
Side jobs
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.

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. Lobbying, political influence or private sector interventions

Change/dynamics
Changes in an organisation or in the environment of an organisation may give rise to instability. 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.

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.

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.

The relevance for each vulnerability enhancing factor is assessed using the a similar scoring model as for the inherent vulnerabilities, estimating the degree of relevance of each factor by awarding 0, 1, 2 or 3 points. The scoring is based on the knowledge and professional judgement of the auditor. It is advised to do the scoring in teams, so team members can challenge and validate each others appraisal.

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

Next the average score per cluster is computed. Finally the result of this process is entered into the form 3, see Annexes.

Keep notes of the discussions and ideas so that you keep track of the background of the scoring to add to the audit file.

6.4 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. Based on the assessment the team can discuss likely integrity breaches and risks and what controls or measures have to be in place. In short by following three steps:

Step 1: determine the profile
Step 2: formulate probable integrity breaches
Step 3: formulate expected management controls / measures

- *Step 1:Profile*

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.

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

The vulnerability profile is incorporated in form 4, see Annexes.

Keep notes of the discussions and ideas so that you keep track of the background of the scoring to add to the audit file.

- *Step 2: Integrity breaches*

Considering the vulnerability profile, what 3 to 5 areas are most vulnerable? Based on the assessment so far one or more integrity incidents are formulated that are likely to occur and

that damage the image of the organisation in such a way that the organisation is no longer able to fulfil its public function properly.

An example of an integrity incident is the event that immigration papers can be bought from certain employees of the immigration office. This facilitates people trafficking and damages the public trust in the immigration office. This step helps to focus on the organisation's main vulnerabilities. Make notes of the ideas and discussions.

- *Step 3: Expected controls*

Considering the vulnerabilities and possible integrity incidents, what specific controls or measures would you expect to be in place? These must be measures of the organisation's management to prevent these incidents happening, but also measures to react to the incident if it occurs, so the damage to the organisation is mitigated. Make notes of the expected controls.

7 Modalities to use this methodology

This method of vulnerability assessment can be used for different purposes. Each purpose requires different ways of data gathering, validation, evaluation/ expressing an opinion and reporting. Each approach also has different implications for the relation with the auditee and other stakeholders.

- *Pre-audit risk assessment on the entity level*

This can be part of the requirement for the auditor obtain an understanding of the nature of the entity/programme to be audited and to conduct a risk assessment or problem analysis. Based on this analysis the auditor can formulate what weaknesses should be expected and what controls to counterbalance these weaknesses.

Depending on how detailed the risk analysis needs to be, the auditor can get his information through desk research, based on e.g. other (internal) audit reports, consultation of experts, press analysis (earlier incidents), complaints (e.g. ombudsman), analysis of social media etc. Also a survey amongst employees is a possibility.
Validation can take place by interviewing of other experts or key figures from the organisation.

Evaluation should take place within the audit team, based on the professional discussion between the team members.

Reporting can be based on the format that is provided with the methodology. Also the outcome of the discussion should be included in the audit dossier.

This approach fits well within the common practices in auditing. However, it does not give many opportunities to transfer the responsibility for both the risk analysis and the quality of the control system to the auditee.

- *Sectoral or government wide risk mapping*

This can be part of the strategic activity and audit planning procedure of a SAI. It will give the SAI an overview of the most vulnerable areas or entities within its remit or within the sector it is reviewing. This will help the SAI to focus its audit activities and prioritize the audit planning. Either on the entity level (what entities are most vulnerable?), on the sector level (what sector is most vulnerable?) or on the process level (what processes should we target in our audits?).

Depending on the end product, the data gathering and ensuing steps can vary from relatively light (if used for internal purposes only) to very thorough (if the risk map is published).

Again the light version can start with using the knowledge of colleagues who are familiar with the sector or entities that are included in the risk map. This knowledge can be extended with some desk research (see above), if required. One step further is to involve experts, who can contribute with their knowledge in workshops. Again one step further is to use a survey. This can be either targeted at the entities themselves, but also perception surveys can be included, where employees and/or users can be asked about their experiences.

The more extensive the approach, the more rigorous the validation needs to be. In the lighter version validation by team discussions or workshops with experts can be sufficient. In the case where surveys are used, validation will take more effort (and time). If the data come from the audited entities themselves verification can take place through sampling. If perception surveys are used also the methodology itself must be scientifically and statistically validated.

Evaluation can again take place within a workshop/ group session for the lighter version, but the survey methodology requires indices that need to be externally validated.

Finally the reporting can take the form of a excel worksheet, showing the total results, to a sophisticated GIS application where survey results are plotted for each entity.

The light version of this approach can fit well within the audit planning procedures, but again it does not give much opportunity to engage the entities and other stakeholders in the integrity approach. However it can be a very good first step.

The survey method requires a lot from stakeholder involvement, is expensive and sophisticated, but offers plenty of opportunity to engage the entities and implement the integrity approach. A big advantage is that, once established, they provide a good basis for benchmarking and monitoring.

- *Self assessment by the public entity itself*

This approach means that public sector entities take on the responsibility for their own integrity management, by conducting a self assessment of their risks and maturity of their controls. This method requires already a maturity of integrity awareness within the public sector. SAINT is an example of using self assessment. This takes the form of a workshop that is facilitated by a trained moderator. The results are used within the entity itself, but may be shared on a voluntary basis.

Part III Annexes

Form 1 Object and processes

The audit object is ***

The organisational objectives and operations are:

- *
- *
- *

The main tasks/processes are:

1)
2)
3)
4)
5)
6)
7)
8)
9)
10)
11)
12)

Notes and first observations:

Form 2 Assessment of vulnerability

1. Check and score vulnerable areas / activities / actions

This table is used to assess whether and to what extent important processes in the organisation are inherently vulnerable.

Compare the information of the audit object with the processes mentioned in the table below and use the following scoring method:

0 = Not important 1 = Relevant 2 = Important 3 = Very important

	Vulnerable areas /activities /actions		**Score 0-3**
Relationship of the entity with its environment	1 Contracting	procurement, tenders, orders, assignments, awards	
	2 Payment	subsidies, benefits, allowances, grants, sponsoring	
	3 Granting / Issuance	permits, licenses, identity cards, authorizations, certificates	
	4 Regulating	conditions of permits, setting standards / criteria	
	5 Inspection / audit	supervision, oversight, control, inspection, audit	
	6 Enforcement	prosecution, justice, sanctioning, punishment	
Managing public property	7 Information	national security, confidential information, documents, dossiers, copyright	
	8 Money	treasury, financial instruments, portfolio management, cash/bank, premiums, expenses, bonuses, allowances, etc.	
	9 Goods	purchasing / selling, management and consumption (stocks, computers)	
	10 Real estate	buying / selling	
Average Score			
Level			

2. Describe and explain shortly the background of the scores.

Form 3 Assessment of vulnerability enhancing factors

1. Check and score vulnerable areas / activities / actions

In addition to the inherently vulnerable areas / activities / actions some circumstances may enhance the existing vulnerability of the organisation to integrity breaches.

Consider the five clusters of examples of vulnerability enhancing factors mentioned in the table below, fill the table and use the following scoring method:

0 = Not important 1 = Relevant 2 = Important 3 = Very important

	Score (0-3)
1. Complexity	
1.1 Innovation / advanced (computer) systems	
1.2 Complex legislation	
1.3 Special constructions (legal / fiscal)	
1.4 Bureaucracy	
1.5 Lobbying	
1.6 Networks of relations	
1.7 Mix of public-private interests (commerce / competition)	
1.8 Need for external expertise	
1.9 Political influence / intervention	
2. Change/Dynamics	
2.1 Young organisation	
2.2 Frequently changing legislation	
2.3 Strong growth or downsizing	
2.4 Privatisation / Management buy-out	
2.5 Outsourcing	
2.6 Crisis (reorganisation, threats with huge impact, survival of the organisation or job at stake)	
2.7 External pressure (pressure on performance, expenditure, time, political pressure, shortages / scarce resources in comparison with duties)	
3. Management	
3.1 Dominant	
3.2 Manipulative	
3.3 Formal / bureaucratic	
3.4 Solistic operation	
3.5 Remuneration strongly dependent on performance	
3.6 Lack of accountability	
3.7 Ignoring advice / signals	
3.8 Defensive response to criticism or complaints	
4. Personnel	
Work environment / Loyalty	
4.1 Pressure on performance / income dependent on performance	
4.2 Low status / lack of esteem/ low rewards / low career prospects	
4.3 Poor working conditions / High workload	
4.4 Group loyalty	
4.5 Power to obstruct	
5. Problem history	
5.1 Complaints	
5.2 Gossip and rumours	
5.3 Signals / whistle blowers	
5.4 Earlier incidents (recidivism)	
5.5 Administrative problems (backlogs, inconsistencies, extraordinary trends etc.)	

2. Fill the table below:

- **Calculate the average score per cluster and the overall average score**
- **Assess the average level (Low ≤ 0.8, Medium 0.8 < >1,6, High ≥ 1,8)**

Clusters of vulnerability enhancing factors	**Average score (0-3)**
1. Complexity	
2. Change/Dynamics	
3. Management	
4. Personnel	
5. Problem history	
Overall average score	
Level	

3. Describe and explain shortly the background of the scores:

Form 4 Vulnerability profile

1. Fill the table below:

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

2. Formulate Integrity breaches that may occur

- ***
- ***
- ***

3. What controls or measures would you expect to counterbalance this (to prevent the integrity breaches from happening or to mitigate the consequences)