# Appendix A:
# **Various forms of fraud and corruption**

As mentioned in subchapter 2.2.1, fraud and corruption can be divided into many different types or categories of acts and practices. Among the various typologies in use, a rather exhaustive one is provided by UNODC[1], and the presentation below is mainly based on this typology:

***Bribery:***

For the purpose of this guide, bribery refers to the act of promising, offering or giving, to a public official – either national, foreign or in a public international organization – money, services or other benefits to persuade her or him do something in return. It also refers to the act of solicitation, that is, to the acceptance by the public official of the money, services or benefits offered.[2] Bribery can take place at both the lowest and the highest levels of government, and it can involve everything from 'small change' to extraordinarily large side payments. According to UNODC, bribery is probably the form of corruption which is most common.[3] Hence, this is probably also what many first and foremost associate with the term 'corruption'.

According to UNODC, bribery can also be divided into various specific types. Two types are further elaborated below, as they illustrate the 'grey zones' between acceptable, unacceptable and criminal behavior:

- The first is trading in influence or so-called 'influence-peddling', where Government insiders, politicians or public officials sell or trade the exclusive access they have to decision makers or their influence on Government decision-making. According to UNODC, influence-peddling must be distinguished from legitimate lobbying or political advocacy.[4] However, the boundaries between what is legitimate and acceptable – and what is not – are not always clear-cut and unambiguous. Influence-peddling take place along a *continuum* which spans from acceptable lobbying to criminal behavior.[5]
- The second is offering or receiving improper gifts, gratuities, favours or commissions. This is central in influence peddling, for example where lobbyists offer or provide various benefits to public officials or elected representatives such as meals and entertainment, trips and other gifts in exchange for the use of their political influence to benefit the

[1] According to UNODC, corruption can be divided into the following categories: 1. 'Grand' and 'petty' corruption; 2. 'Active' and 'passive' corruption; 3. Bribery; 4. Embezzlement, theft and fraud; 5. Extortion; 6. Abuse of discretion; 7. Favouritism, nepotism and clientilism; 8. Conduct creating or exploiting conflicting interests; 9. Improper political contributions. (UNODC, 2004, pp. 10-16.) For further reading, see also, among others, UNODC, 2005, pp. 21-27, and UNODC, 2003, UN Guide for Anti-Corruption Policies. [Online] Available at www.unodc.org/pdf/crime/corruption/UN_Guide.pdf [Accessed on 22 February 2011], pp. 28-34.
[2] The full definitions of bribery of a) national public officials, and b) bribery of foreign public officials and officials of public international organizations are found, respectively, in articles 15 and 16 of the United Nations Convention against Corruption (UNCAC).
[3] UNODC, 2004, p. 11.
[4] UNODC, 2004, p. 12.
[5] McPherson and MacSearraigh, 2007, p. 201.

former or his/her clients.[6] UNODC points out that such improper benefits are difficult to distinguish from bribery as links are always developed between benefits and results.[7] However, the perceptions as to what qualifies as reasonable and appropriate gifts, payments, etc. differ very widely between various cultures. This form of bribery can therefore be difficult to address.[8]

***Embezzlement:***

This refers to the misappropriation or stealing of money, property or other public assets by public officials who are not entitled to these assets, but have been entrusted to them through their position or employment. 'Theft' is also associated with embezzlement, but has a wider meaning than the latter concept, as it also includes the stealing of property or other assets which have not been entrusted to the person in question.[9]

***Extortion:***

In contrast to bribery, extortion or blackmailing involves the use of negative incentives such as threats of exposure of harmful information or threats or use of violence to achieve cooperation. Government officials and public servants can both commit extortion or be the victims of it. In some cases, the difference between extortion and bribery may only depend on the extent of coercion involved. Furthermore, through the acceptance of a bribe, a public official also becomes much more vulnerable to extortion.[10]

***Intentional misrepresentation and deception:***

This refers to the giving or receiving of misleading or false information to obtain an unjust or illegal advantage. In contrast to embezzlement, intentional misrepresentation and deception is used to induce the owner of money, property or other assets – here: the State – to relinquish it voluntarily. It can be commited both internally, for instance when public officials create artificial expenses, and externally, for example when individuals, groups, or companies are receiving public funding on false premises.[11] This type of abuse of public funds and/or office is perhaps what is most commonly associated with the term 'fraud'.

***Abuse of discretion:***

Abuse of entrusted discretion for private gain may be involved in various cases of fraud and corruption in the public sector. For instance, a government official responsible for public procurement may abuse her or his discretion by purchasing goods and services from a firm where she or he has vested interests or by altering rules and criteria pertaining to the use of particular areas so that the value of their personal property increases. This type of fraud and corruption is frequently related to bureaucracies in which individual discretion is wide and the

[6] Kupferschmidt, David, 2009. Illicit Political Finance and State Capture, International Institute for Democracy and Electoral Assistance. [Online] Available at www.idea.int/resources/analysis/upload/IDEA_Inlaga_low.pdf [Accessed on 22 February 2011], p. 35-36.
[7] UNODC, 2004, p. 12.
[8] Pope, Jeremy, 2000. Confronting Corruption: The Elements of a National Integrity System, TI Source Book 2000, Transparency International. [Online] Available at www.transparency.org/publications/sourcebook [Accessed on 24 January 2011], pp. 8-9.
[9] UNODC, 2004, pp. 13-14.
[10] UNODC, 2004, pp. 12, 14-15.
[11] See, among others, UNDP, 2010, p. 8; UNODC, 2004, p. 14.

surveillance and accountability structures are weak, and/or rules and procedures which are so complex that they undermine the effectiveness of the internal controls and accountability mechanisms that are in place.[12]

***Favouritism, nepotism and clientilism:***

In general, this form of fraud and corruption also involves abuse of discretion. However, this type of abuse is not initiated by the self-interest of the government official in question, but by the interests of relatives, friends, tribe or clan members, fellow party members, etc. Among other things, it involves the exploitation of power and authority to procure jobs and positions for relatives irrespective of their objective qualifications (nepotism).[13] According to UNODC, there is a number of States which have not criminalized the conduct of favouritism, nepotism and clientilism.[14] Hence, as with influence-peddling and the offering or receiving of improper gifts etc., this type of fraud and corruption also illustrates the 'greyzones' between acceptable, unacceptable and criminial behavior.

***Improper political contributions:***

As with other attempts to affect political and other important decisions by government officials, donations or other contributions to political parties also take place along a long continuum which spans from legitimate contributions to attempts at improperly influencing specific decisions by a party or its members in the present or in the future. Consequently, due to the many 'greyzones' involved, this type of fraud and corruption has proved very difficult to deal with in practice. One way to prevent improper use of political contributions is to provide for transparency through disclosure requirements, so that both the donor and the recipient are known to the public and, hence, politically accountable. Another approach is to stipulate an upper limit for the size of contributions from individual donors.[15]

[12] UNODC, 2004, p. 15.
[13] UNODC, 2004, p. 15; UNDP, 2010, p. 8.
[14] UNODC, 2005, pp. 26-27.
[15] UNODC, 2004, p. 16.

# Appendix B:
# **The 'Code of Conduct'-concept**

The preferences and value judgments of public sector employees – and thereby their standards of conduct – are determined by their ethical values and personal and professional integrity. Hence, since the 1990s, in addition to prevention and detection of fraud and corruption, more attention has also been drawn to the importance of ethical conduct in the public sector. Public ethics are a precondition for, and support the confidence of the people in the public sector and are at the core of good governance.[16]

Consequently, measures to prevent fraud and corruption can be underpinned by more universal standards of ethics and behavior to encourage high quality in public services, good relations between public sector employees and those they work for, i.e. the people, as well as efficiency, determination and spirit. Such principles can, at the same time, both encourage a culture of professionalism in the public sector, and also strengthen the expectation among the general public that the standards are high in this sector. The principles should therefore ideally be reflected in written documents such as a Code of Conduct (CoC) or a similar document, and it is also advisable that this document is made public.[17]

In addition to the Executive branch of government, such ethical standards are also relevant for the Legislature[18], the Judiciary[19], as well as the Supreme Audit Institution[20].

The basic purposes of a CoC are, among other things: (i) To make it clear what should be expected of individual employees or a group of employees, thereby contributing in promoting basic values which restrain fraud and corruption; (ii) To form the basis for training of employees, discussion of standards and, when required, adjustment of standards; (iii) To form the basis of disciplinary reactions, including discharge, in instances where employees contravene or fail to satisfy a standard as stipulated.[21]

As to the more general content, a CoC normally prescribes common standards of conduct in line with fundamental ethical principles such as independence, integrity, impartiality, transparency, accountability, justice, responsible use of public resources, diligence, loyalty towards the organization, and propriety of personal conduct. More or less, all these principles have their sources in legislation, delegated legislation or regulations, and contract law. Hence, a CoC will often draw most of its basic principles from existing legislation, and supplement it as appropriate. Where necessary, a CoC can be 'tailor-made', that is, include more specific standards which apply to specific groups of employees. At the same time, however, it is important to ensure that such specific standards are not in conflict with more general standards which already apply in legislation or elsewhere.[22]

---

[16] INTOSAI GOV 9100, pp. 10, 17.
[17] UNODC, 2004, p. 136; INTOSAI GOV 9100, p. 18.
[18] UNODC, 2004, pp. 180-183; Pope, 2000, pp. 52-53. See also Inter-Parliamentary Union, 2001: Recommendation on the Role of Parliament and Supreme Audit Institutions in combatting corruption. Approved at the Session on the role of parliaments and supreme audit institutions in the fight against corruption, held during the Second Global Forum on Fighting Corruption and Safeguarding Integrity, The Hague (Netherlands), 28-31 May 2001. [Online] Available at www.ipu.org/splz-e/hague01-rcm.htm [Accessed on 4 April 2012].
[19] UNODC, 2004, pp. 112-15, 119. Pope, 2000, p. 69.
[20] See ISSAI 30 Code of Ethics.
[21] UNODC, 2004, p. 133.
[22] UNODC, 2004, pp. 133-135.

Central elements in a CoC for public officials when it comes to fraud and corruption could be, inter alia: 1. Standards concerning impartiality; 2. Standards concerning conflicts of interests; 3. Standards concerning administration of public resources; 4. Standards concerning confidentiality.

*1. Impartiality:*

Impartiality is important to the proper and uniform conduct of public tasks and to make sure that the public is confident in them. In general, the impartiality principle applies to any public employee who makes decisions. However, it could be argued that stricter or more specific requirements normally should apply to more influential or powerful decision-makers, such as public servants at senior level, judges and office holders in the legislative or executive branches of government. In essence, impartiality demands that decisions are made on the basis of facts only, i.e. without the possible influence of extraneous or immaterial considerations.[23]

*2. Conflicts of interests:*

Among other things, the extraneous and immaterial considerations just mentioned may arise when the private interest of a public official conflicts with her or his public duty. Hence, a central element of a CoC is to address such conflicts. One general requirement in this regard is for public officials to steer clear of undertakings which might result in conflicts of interests. For instance, officials responsible for decisions which affect financial markets should be very cautious with personal investments at the same time. Another requirement is that public employees avoid conflicts of interest by pleading partiality or prejudice in situations where they directly/indirectly can affect their own personal interests.[24]

A third requirement is that public officials should not accept gifts, favours or other benefits.[25] In more serious cases, where a direct link can be proved between a gift and a decision, bribery provisions in the penal code may apply. However, usually, the link is more subtle. Therefore, to prevent such situations from arising and make sure that there is no impression of partiality, the safest measure would probably be to have a general prohibition in the CoC on the acceptance of gifts, benefits, etc. with exceptions only for very small gifts, i.e. gifts of 'symbolic value'. In cases where government officials – in particular situations – nevertheless are permitted to accept gifts, the CoC can also stipulate that information regarding the type and value of the gift and the identity of the giver be disclosed, so that the question of whether the gift is inappropriate or not can be subject to an independent assessment.[26]

Finally, a fourth requirement is that officials disclose all their incomes, assets, business interests etc. which may raise conflicts. Often, this is reflected in provisions stipulating a general disclosure when officials are beginning in their new job and on a regular basis after that. As part of this, there are also frequently provisions which prescribe that potential conflicts of interests due to officials' financial positions should be disclosed as soon as they become apparent. Central questions in this regard are, inter alia: Who should receive the disclosures, and to what extent should these be made public? When it comes to non-political officials, i.e. civil servants – at what levels of seniority should these also be required to

[23] UNODC, 2004, p. 136.
[24] UNODC, 2004, p. 137.
[25] See also appendix A for a brief account of this type of fraud and corruption.
[26] UNODC, 2004, p. 137

disclose this type of information?[27] On a general basis, however, it can be suggested that disclosure becomes more important, the higher the level of the official in question. The same argument goes for the degree of publicizing of officials' financial positions.

*3. Administration of public resources:*

Officials responsible for managing public funds or assets may represent a particularly high risk of fraud and corruption, as they normally are in a position to allocate financial or economic benefits and to manipulate systems which are established to prevent or detect irregular practices in this area. Normally, these are officials who make decisions relating to expenditures, procurement of goods or services, management of public property or other assets – in addition to those responsible for the supervision and auditing of such officials. Hence, stricter rules may be required for officials in this category, although with many of the same characteristics as the more general rules pertaining to conflicts of interests. In addition to rules which prescribe avoidance or disclosure of real or possible conflicts of interests, standards concerning administration of public resources may therefore also focus specifically on maximizing the public benefits of any expenditures at the same time as costs, waste and inefficiency are minimized.[28]

*4. Confidentiality:*

Government officials and civil servants often have access to a broad spectrum of sensitive information – information which may be misused for fraudulent or corrupt purposes. Hence, a CoC should also ideally contain rules relating to confidentiality. Such rules may include, inter alia, secrecy declarations which provide that sensitive information be kept secret unless otherwise required; classification systems to give guidance to officials on what should be kept secret or not, and how; prohibitions on the use or disclosure of confidential information to make profits or to gain other benefits; prohibition on the use or disclosure of sensitive information for a suitable period after the official in question has left the public service.[29]

***Implementation of a Code of Conduct:***

To be effective, a CoC also must be properly implemented in the organization in question. To achieve this, there are several prerequisites which ideally should be in place. First, to ensure that the CoC adequately addresses the possible situations and aspirations of employees at all levels in the organization, and that everybody has a feeling of ownership of the CoC, staff at all levels should ideally be involved in its preparation. Second, a CoC must be combined with an ethics programme which both includes an effective implementation plan and a strong dedication to make sure that the plan is fulfilled. This may include a combination of both 'soft' and 'hard' measures.[30]

As to the 'soft' measures, these should ideally include as many positive incentives as possible to ensure that every employee becomes aware of the CoC, and to encourage compliance. More specifically, this includes information and education schemes, and regular training on

[27] UNODC, 2004, p. 137; Pope, 2000, pp. 187-88.
[28] UNODC, 2004, p. 138.
[29] UNODC, 2004, pp. 138-139.
[30] Pope, 2000, p. 181; UNODC, 2004, p. 146; Dye, Kenneth M. (2007) Corruption and Fraud Detection by Supreme Audit Institutions, pp. 318-19, in: Shah (ed.), 2007.

real life ethical dilemmas and on the steps every employee can take to make sure that their colleagues also comply with the CoC.[31]

The 'hard' measures, on the other hand, are aimed at effective enforcement and refer to clear procedures and sanctions to be applied in case of breaches of the CoC. To ensure effective implementation, integrity seminars should therefore also – in addition to the positive incentives – focus on the consequences if employees are found to violate provisions of the CoC. Moreover, to ensure that the disciplinary procedures are carried out in a fair and proper manner, it is advisable that there are tribunals or similar bodies in place, to investigate complaints, adjudicate cases and decide on and enforce appropriate measures. Finally, it could also be argued that disciplinary procedures and their results should be transparent to ensure that the employees involved are fairly treated and to assure other employees and the general public that the CoC is applied fairly and effectively.[32]

Third, to support implementation, the CoC should also ideally be formulated with clarity and in a way which makes it easy to understand both for those who are supposed to comply with it, i.e. the 'insiders', and the citizens who they serve, i.e. the 'outsiders'. Fourth, to provide guidance to employees on how the CoC should be interpreted in particular instances – so that breaches and disciplinary actions can be avoided – it is advisable that consultancy mechanisms are in place, through a dedicated individual or body. Finally, to improve effectiveness, it also seems appropriate to disseminate and promote the CoC widely, both throughout the public entity or sector in question and among the general public, so that everybody is informed of its contents.[33]

[31] UNODC, 2004, pp. 146-147; Pope, 2000, p. 182.
[32] UNODC, 2004, pp. 146-48.
[33] UNODC, 2004, pp. 135, 146-47; Pope, 2000, p. 182.

# Appendix C:
# Fraud- and corruption-related research[34]

In practice, fraud and corruption or forensic auditing often involves a broad spectrum of activities and methods which bear resemblance to the methods applied by both police investigators and investigative journalists. Fraud- and corruption-related research - whether this is done by searching certain online data bases or performing general Internet searches - is a central part of this.

Inter alia, this type of research has the following three advantages: First, to a large extent, data base and general Internet searching can be carried out *in secret*, i.e. without involving the suspect and/or other persons[35]. Secondly, this type of research does not necessarily require a great deal of resources. Thirdly, information obtained from public registers is generally considered to be correct and updated.

In general, fraud- and corruption-related research can be divided into *1) closed source research* and *2) open source research*.

## 1. Closed source research:

Depending on their mandate and technical capabilities, many SAIs have access to various data bases which normally are closed to the public at large. These registers usually contain (sensitive) information about individuals. From a forensic auditing perspective, the following types of data bases/directories - among others - are relevant:

**National population register/directory of residents:**

A national population register normally contains basic information about a country's residents. Depending on the country in question, the population register may include information such as:

- Personal identity number
- Family relations (parents, siblings, children, married couples)
- Changes of address domestically and abroad, mailing addresses and blocked addresses
- Changes of marital status
- Name changes
- Citizenship
- Working- and residence-permit

Combined with data from other registers, details from the national population register may for example confirm or reject suspicions on possible conflicts of interest by providing

[34] Where not otherwise stated, this appendix is mainly based on the following guideline produced by the Office of the Auditor General of Norway: "Veiledning i bruk av transaksjonsanalyse til vurdering av risiko for misligheter", December 2011. Hence, the guidance provided in this appendix is to a large extent based on experiences from Norway. Both the content of, and the access to various public registers/directories may vary a lot from country to country around the world.

[35] Note that fraud and corruption research may also involve offline searches in public and/or organizational archives. While such research can be performed discreetly, one must take into consideration that personnel working in the archives will often need to be consulted.

information on family relations. More specifically, it may confirm or reject suspicions that a government official is abusing her/his position by favouring members of her/his family.

**National employer/employee register:**

In an employer/employee register, the auditor may find information on present and previous employment for individuals and companies. Person searches may require personal identity numbers, while searches for companies may require business register numbers. Data from this type of register may inter alia be used to confirm or reject suspicions on possible conflicts of interests, such as former colleagues doing business with each other.

It should be noted that some countries may not have separate data bases dedicated to storing employment information.

**Other closed sources:**

To the extent that such information is available in the country in question, *transaction data* from the foreign exchange register, *tax returns* and supporting documentation, and *personal credit ratings* can also be very useful for the auditor. Normally, however, access to such data may require specific requests to other control authorities such as the tax and customs authorities.

To get the full overview of roles and relations, it is often necessary to combine information from various data bases. Auditors should be aware that the use of closed source data bases is regulated by national legislation. Therefore, it is likely that requirements as to the use and storage of such information will vary from country to country, and from register to register. Generally, the auditor must pay attention to data protection of all sensitive and personal information. Thus, auditors should exercise due professional care and caution, and consult appropriate legal counsel whenever necessary, cf. paragraph 4.7 in ISSAI 300.

## 2. Open source research:

As mentioned, many of the activities and methods applied in forensic auditing may have similarities with the methods applied by investigative journalists. As journalists normally do not enjoy the same access to registers and public records as SAIs and other control authorities, they have to find more or less creative ways of obtaining information through open sources instead. Hence, investigative journalists may have a lot of knowledge and experience on efficient and effective online research which may be of value for public sector auditors as well. For instance, many countries have organizations that provide reports on methods applied in particular fraud and corruption cases. In addition, there are several international organizations, such as *The Centre for Investigative Journalism (CIJ)*, which also may provide a variety or resources, including links to other investigative organizations at a global, regional and national level, as well as guidelines on investigative online research.[36]

Below, open source research will be divided into *a) business register searches*, *b) national registers of property/land and movable property searches*, and *c) general Internet research.*

[36] See www.tcij.org. Among other things, the following tool can be downloaded from this website: Dick, Murray, 2011. Investigative Online Search: An Introduction. Available on www.tcij.org/sites/default/files/u4/CIJ_Investigative_Online_Search_26_05_11.pdf.

**a) Business registers:**

Business registers normally contain key information on companies, their administration, board of directors and owners, as well as key financial data. Furthermore, they may also provide annual reports and accounts. The bullet points below contain some of the key elements included in such registers, as well as associated questions which may be relevant to ask when researching possible fraud and corruption. While the bullet points mainly contain references to the procurement area for example purposes, the same information may be relevant to a number of other areas, such as sales and disposals, reimbursements and grants:

- *Shareholders, Chief Executive Officer (CEO) and Board of Directors:* Provides information on the administration, composition of the board and ownership in the company.

  After identifying key persons in an organization, the next step could be to further examine the various roles and networks of these persons. For instance:

  - Do employees in the audited government entity have ownership interests and/or other roles in companies which are doing business with this entity?

  - Are employees in the government entity closely connected to people in particular companies through marriage, family, previous employment, etc.? (May also require access to national directory of residents and national employer/employee register).

- *Date of establishment:* Is the researched supplier company established just prior to, or shortly after the first invoice was sent to the entity being audited? If so, this may indicate that the company has been established with the sole purpose of siphoning off money from the government entity in question.

- *Date of liquidation:* If a supplier company continues to invoice a government entity after the former has been liquidated, there is a substantial risk that the 'supplier' is being paid for goods/services which never have and never will be delivered.

- *Number of employees:* If a supplier company has few or no employees, while at the same time delivering goods and/or services that imply a larger number of employees, it may be relevant to look for possible subcontractors and try to reveal the reason why the subcontractor is not known to the government entity.

- *Branch:* Does the stated company activity (branch) match the type of goods/services being supplied? If not, one could question the basis upon which the company was engaged in the first place.

- *Income and accounts:* Information from a company's annual accounts is often relevant in fraud and corruption research. First of all, the auditor should inquire whether approved accounts are at all available (in so far as the company is obliged to submit such accounts). Next, the auditor could inquire information about:

  - Shareholders
  - Board of Directors

- Financial development
- Core activities
- Main income source
- Major expenses
- Major disposals
- Etc.

In for example a transaction analysis of procurement data (see appendix D), annual income may be compared to the total amount invoiced during the research period. If the total amount invoiced equals between 60 to 100 % of the annual income, this may indicate a dependent relationship between the company and the government entity.

- *Audit:* Has the (private) auditor at the supplier company presented a negative opinion? Is there a frequent replacement of auditors in the company? In jurisdictions where legislation allows small (limited) companies to choose not to have their accounts audited - has the company in question chosen this option? If the answer is yes to any of these questions, this normally calls for further inquiries by the auditor.

- *Announcements:* These provide a historical account of changes of company name, board of directors, CEO, branch, business address and/or auditor, as well as information of liquidation, bankruptcy, mergers and divisions. This may also provide valuable information to the auditor on roles, relations and interests.

*Foreign business registers:*

In many instances, it may be required to follow money flows to companies registered abroad. In such instances, the auditor should approach national business registers. However, both the access to, and the quality of, company information may vary greatly from country to country. Furthermore, not all information is provided free of charge. In some cases, it may be costly to obtain company data.[37] In addition, there may be language challenges and significant differences in how jurisdictions are administered and organized. Hence, co-operation with SAIs in other countries may be very helpful when performing fraud and corruption research.[38]

**b) National registers of property/land register and movable property (normally open source):**

*National property/land register:*

Among other, a national property/land register normally provides information about the ownership of registered properties in a country. This information may be used to confirm or

[37] See Radu, Paul Christian, 2009. Follow the Money: A Digital Guide for Tracking Corruption. Romanian Centre for Investigative Journalism. [Online] Available at http://issuu.com/kijf/docs/follow_the_money_web [Accessed on 11 July 2012]. The chapter on "Online Company Research Tools", pp. 27-48, provides information both on unified databases, i.e. databases which have data from different sources in various countries, as well as information on national business registers in several countries around the world.

[38] As an alternative, if the auditor knows the exact spelling of a key phrase or key phrases in the local language - and if necessary, the type of letters - she or he may perform searches using these key phrases and then translate the top findings through translator programmes available on the Internet. Although the quality of such translations may be rather low, they still may give the auditor a first indication as to whether she/he is 'on the track of something' or not. If the material seems interesting, the auditor may then forward it to a professional translator so that it can be further scrutinized in the next round.

reject suspicions of possible illicit enrichment.[39] Combined with other information, details from this type of register may also confirm or reject suspicions on possible conflicts of interest in connection with sales of public property by providing information about the buyer and seller.

*National register of movable property:*

As for the national property registers, this type of register may also provide information which confirms or rejects suspicions on possible illicit enrichment.

**c) General research on the Internet:**

General Internet research includes everything from using search engines such as Google combining various phrases and names of persons, companies, organizations, addresses, etc., to searches in local media and branch journals/industry publications. When performing Internet research in a foreign country, it is important to remember that local sources may be more accurate and informative than publications covering a larger region.

Some Internet search tools worth mentioning for forensic auditors include (i) *interactive maps* and (ii) *telephone directories*.

*(i) Interactive maps* such as Google Earth provide satellite images and street views which may inter alia be used to check the authenticity of addresses. For instance, if a company has presented itself as a large, well-established and professional production company and it turns out the company's only address is in a small office building alongside a large number of other companies, this may give reason for suspicion and further inquiries. Moreover, the surroundings of the building(s) in question may also provide valuable information - do they correspond with the type of services/goods the company/organization/person is supposed to deliver, or with the operations which are supposed to be carried out in this area?

*(ii) Telephone directories* - both yellow and white pages - may also be useful to the auditor. When researching a supplier company, for instance, searches in local and/or international directory services can provide information as to the availability of the company. If the company is not listed in any major directories, this may give reason to question whether the company is genuine or not. Or, if the phone number of an organization receiving grants from/a company providing goods/services to the public entity being audited is registered at a different address than what appears from the official documents, this may also call for further inquiries. In both cases, the auditor could inquire whether any employees at the public entity involved in the grant/procurement are listed at the same address as the 'unofficial' organization/company address.

In general, the following questions - among others - may be relevant to pursue when performing general Internet searches:

- Is the company in question well marketed?
- Is the company-/organization-address also a private address?

[39] "Illicit enrichment" refers to a substantial increase in the standard of living and/or the assets of a (former) public servant or government official which is significantly disproportionate to her or his known past or present legitimate income, and which cannot be sufficiently accounted for.

- How is the company/organization described/referred to in the media? (Negatively/positively/not mentioned at all?)
- Does the company/organization have its own website? If so, how does this website appear when it comes to information, transparency and professionalism? Is it regularly updated?
- Is the company listed on any sort of official 'black list'/market warning issued by a financial surveillance (or similar) authority?
- Is the company/organization/person mentioned in publications related to legal proceedings?
- Does the information found on the Internet concerning companies/organizations/persons correspond with information found through other sources?

The value of this type of research will largely depend on the auditor's ability to find information efficiently, to understand what the information collected indicates, and to document it in light of the objectives of the inquiry. Finding information which indicates or, more rarely, confirms/rejects suspicions of possible fraud and corruption entails being able to foresee alternative scenarios and think creatively about what possibilities exist.

Hence, as with fraud and corruption risk assessments presented in chapter 4, research is often best carried out by a team as opposed to by one auditor alone, both when it comes to sharing the workload and obtaining various inputs deriving from different background knowledge, experience and skills.

# Appendix D:
# **Transaction analysis**[40]

Transaction analysis is a computer-assisted audit technique which can be used to assess the risk of fraud and corruption in a particular entity. The technique is relevant both for financial and performance auditing. In financial auditing the technique may be used in all stages of an audit cycle.

The purpose of a transaction analysis focusing on fraud and corruption is to systematize transactions according to specific selection criteria that can represent 'red flags'. Hence, the analysis can also be instrumental in detecting fraud and corruption by identifying unusual transactions, unusual circumstances related to transactions, as well as unusual transaction patterns.

On a global level, computer-assisted audit techniques are referred to as Computer Assisted Audit Tools and Techniques (CAATTs)[41]. CAATTs include a variety of computer-based tools and techniques for the analysis of large amounts of data with the aim of identifying irregularities. Experience has shown that CAATTs are instrumental in improving and increasing the efficiency of audits, and in guiding them towards important risk areas.

While there is a potential for increased efficiency, one should be aware that transaction analyses often can be time consuming and be technically challenging. This implies that the auditor, especially in the beginning, may have to ask for assistance from specialists in this field.

Having a *broad perspective* and the ability to *see 'the big picture'* are critical success factors for an effective transaction analysis. It may often be tempting to initiate substantial inquiries as soon as the first irregularities are discovered. However, if this is done too early, there is a risk that time and resources are spent on examining cases with low materiality and/or which are so-called 'false positives'. Hence, more thorough inquiries should normally be initiated after the transaction analysis is finalized, or possibly in parallel to the finalization of the analysis.

A transaction analysis can be carried out with minimal or no involvement by the entity in question. Therefore, as mentioned, this technique is not only appropriate for risk assessments, but also for particular inquiries of possible fraud and corruption where it is desirable to analyze data without the entity or possible suspects being aware of this, i.e. *tactical considerations*.

Areas which are suitable for transaction analysis are, inter alia, procurements, sales and disposals, grants, salaries, refunds and inventories.

[40] This appendix is mainly based on the following guideline produced by the Office of the Auditor General of Norway: "Veiledning i bruk av transaksjonsanalyse til vurdering av risiko for misligheter", December 2011.
[41] See for instance the websites of The Institute of Internal Auditors (www.theiia.org) and the American Institute of Certified Public Accountants (www.aicpa.org).

**Use of software tools:**

The larger the number of transactions, the more beneficial the use of computer assisted tools for the analysis. Depending on their access and technical infrastructure, transaction data can often be collected by the SAI itself, but in some instances the data sets must be obtained through special orders to the entity in question.

Various software tools are available for auditing purposes, several of which can be used for detecting possible fraud and corruption. Irrespective of the software programme used, it is advantageous if the programme can import many different data formats. Generally, all sorts of electronic data can be systematized (not only transactions) according to the same methodology, but the selection criteria will depend on the area chosen for examination.

If a risk assessment scheme already has been filled out (see chapter 4) for the entity in question, it may be useful to use this as a basis for the transaction analysis. Inter alia, the scheme is supposed to include descriptions of possible methods for carrying out fraudulent and corrupt acts, and through the transaction analysis the auditor can examine further whether the methods suggested in the scheme actually represent a real risk. Moreover, the auditor may also get an idea of which fraud and corruption methods appear to be most relevant.

**Methods for extracting and systematizing data - using procurement data as example:**

The risk of fraud and corruption is often present in the procurements area. Examples of red flags which can be detected in a transaction analysis include:

- Breaches of controls and procedures;
- Private use of entity resources;
- Identification of close relations between employees and suppliers (conflicts of interests);
- Large payments to small businesses run by one person or a limited number of people;
- Payments to offshore companies and tax havens;
- Lack of transparency concerning particular suppliers;
- Exceptionally beneficial terms for particular suppliers (as to deliveries, payments, etc.)

A transaction analysis uses financial data from processes such as Accounts Payable, Accounts Receivable, Travel Expenses and General Ledger. For procurements, it is particularly relevant to extract data from the Accounts Payable and possibly also from the General Ledger. In the table below, various selection criteria and the possible red flags these criteria are based on, will be presented:

| **Selection Criteria** | | **Purpose/red flags/what the auditor is looking for** |
|---|---|---|
| 1 | Sequential invoice numbers | • Suppliers dependent on the government entity for income;<br>• Employees favourizing particular suppliers;<br>• Employees or people closely connected to them have interests in a company which is doing business with the entity;<br>• The choice of supplier is based on acquaintance or close relations rather than professional competence and competitive tenders; |

| | | |
|---|---|---|
| | | • Split purchases to avoid stricter rules and procedures applying to purchases above a certain threshold |
| 2 | Low invoice numbers | • Suppliers dependent on the government entity in question for income;<br>• Unusual suppliers;<br>• Newly set up suppliers |
| 3 | Unusual invoice numbers (letters, dates, etc.) | • Goods and services purchased from non-approved/unregistered suppliers;<br>• Procurements not in line with approved contracts |
| 4 | Lacking invoice number | • Goods and services purchased from non-approved/unregistered suppliers;<br>• Procurements not in line with approved contracts |
| 5 | Round sums | • Unspecified invoices;<br>• Invoices lacking supporting documentation;<br>• Fictitious invoices;<br>• Payments to 'intermediaries', consultants, 'facilitators', agents and external experts;<br>• 'Hidden' bribes |
| 6 | Identical/similar information on the supplier (name) | • Suppliers invoicing for the same product/service from different companies;<br>• The same persons are behind several - but apparently independent - deliveries under a large public procurement scheme;<br>• The need for procurement of external services is defined by external suppliers/consultants already working on contract for the government entity |
| 7 | Nationally registered branch of a foreign company and potential 'PO Box companies' | • 'Hidden' kickbacks;<br>• 'Hidden' bribes;<br>• Money laundering;<br>• Payments to criminals;<br>• Payments to unknown recipients |
| 8 | Offshore companies and tax havens | • Payments to unknown recipients;<br>• Uncontrolled payments;<br>• 'Hidden' kickbacks;<br>• 'Hidden' bribes;<br>• Money laundering;<br>• Payments to criminals;<br>• Payments to agents |
| 9 | Large year-end transactions | • Rush payments;<br>• Uncontrolled payments;<br>• Payments registered within the wrong period;<br>• Available credit time not utilized;<br>• Fictitious invoices;<br>• Over-invoicing |
| 10 | Payment date before invoice date | • Unauthorized payment;<br>• Unusually close relations between employee and supplier;<br>• Suppliers are paid for goods/services which have not |

| | | |
|---|---|---|
| | | been delivered;<br>• Fictitious deliveries |
| 11 | Early payment | • Exceptionally beneficial terms for particular suppliers;<br>• Unusually close relations between employee and supplier |
| 12 | Suppliers with two or more bank accounts | • Employees are channeling payments to themselves or an account which they control;<br>• Payments to third parties not identified in supporting documentation;<br>• Payments to accounts not specified in contracts/supporting documentation |
| 13 | Duplicate invoicing | • Forged invoices without corresponding delivery of goods or services;<br>• Financing of bribes |
| 14 | Double-payment (one invoice is paid twice) | • Unlawful payment which is deliberate |
| 15 | A large number of re-entries and corrections | • Invalid/unauthorized payments |
| 16 | Level of payment identical to or just below the critical threshold set for public procurement | • Split purchases to enable approval by unauthorized personnel;<br>• Split purchases to hide larger purchases from a single supplier |
| 17 | Entries on Saturdays and Sundays | • Unusual or uncontrolled payments |
| 18 | Entries during holiday season | • Unusual or uncontrolled payments |

When the relevant data have been extracted by the software programme, it is advisable to export these data to a spreadsheet like for instance Excel for further editing. Fields which are useful for further editing and analysis are, inter alia:

- Supplier-number/supplier-ID
- Supplier name
- Supplier address
- Supplier invoice number
- Supplier invoice date
- The entity's internal voucher number
- The date of payment from the entity
- Invoice amount
- Total amount for the relevant period

In addition, a list showing the size and rank of all suppliers (from the largest to the smallest) should be extracted. In this context, the size of the supplier equals the sum of invoices issued during the period being analyzed. The list should contain:

- The internal ID-number and name of supplier
- Total value of invoices per supplier
- Total volume of invoices per supplier

- Supplier address and business (organization) number

If possible and/or relevant the list also could include information on which departments in the public entity in question are receiving invoices from the respective suppliers.

**Further analysis of the extracts and identification of possible red flags indicating fraud and corruption:**

In a transaction analysis 50-80 transactions are normally selected for further scrutiny. The number of transactions selected may vary depending on the size of the entity. The transactions are selected using professional discretion and with an aim of finding examples on high risk of fraud and corruption and weak internal controls. In addition, they are intended to illustrate the different red flags which characterize the various data extracts.

Experience has shown that it is difficult to analyze the data only by studying them in electronic format. Hence, to get a good idea of the various transaction patterns it is advisable to make printouts of the extracts from the spreadsheet, and place these in binders. Fields chosen for further analysis should ideally be shown as *one transaction along a single line* in an A4 sheet lying down. Furthermore, transactions which the auditor wishes to examine further may for instance be marked with a colour marker pen, so that it is easier to keep track of the most relevant transactions during the examination of the printouts.

To make an adequate selection of transactions it will usually be necessary to see the extracts in connection with each other. The more extracts one and the same auditor has examined, the easier it will be for her or him to detect the most important red flags. If the auditor in the analysis of i.a. round sums identifies certain transactions which are potentially interesting for further scrutiny, it will also be relevant to look at other indicators in other extracts to 'complete the picture'. Other extracts may for instance show that the rounded sums are just below the threshold where stricter rules and procedures apply, that they are paid during holiday seasons, and that the receiver has a PO Box address abroad.

At the same time it can be useful that more than one person examines the same extracts, or - as a minimum - that several people co-operate on analyzing them. This to ensure that important risk elements are identified, and that the transactions selected are relevant for the further work on assessing the risks of fraud and corruption.

In the analysis of extracts it will also be relevant to identify the so-called 'false positives', that is, findings on selection criteria which do not represent a potential risk of fraud and corruption. Normally, the extracts will contain far more transactions than will be relevant to examine further. One extract may for instance contain approx. 1000 transactions, where perhaps only 100 are relevant when it comes to the risk of fraud and corruption. Moreover, these 100 transactions will again, most likely, be spread over a much smaller number of recipients.

**Further inquiries of red flags:**

On the basis of the examination and analysis of transactions, the auditor selects a few recipients for further inquiries. In these inquiries the auditor both collects internal documents from the entity in question, as well as information from publicly accessible registers and other sources on the internet. In accordance with the 'due care'-principle, cf. paragraph 4.7 in ISSAI

300, all inquiries should be carried out discretely, and information treated confidentially. Should it be necessary to involve one or more persons in the entity to get access to relevant information, it is important that the auditor aims to avoid unwarranted suspicion and unsupported conclusions. If it is necessary to move an inquiry into an open investigation (e.g. interviews of informants and/or suspects), this must only be done after sufficient background material has been collated.

The sources used for transaction analysis and related inquiries are, inter alia:

- Financial data from the accounting system of the entity (regarding recipients of payments and transactions)
- Copies of payment vouchers obtained from the entity (invoices with enclosures are obtained for procurements and revenues)
- Other information obtained from the entity (information regarding orders, contracts, routines, protocols, written correspondence, etc.)
- Publically accessible information on companies (see appendix C)
- The national population register (see appendix C)
- Employer and employee register (see appendix C)
- The telephone directory and other information services (see appendix C)
- General information on the internet (see appendix C)
- The public postal records of public entities

Inquiries in connection with a transaction analysis may potentially comprise many different information sources. However, before the auditor has obtained a general view of the most important risks and possible weaknesses in the internal controls, the inquiries should primarily focus on the following elements:

- The basis for the transaction
- Roles and ownership in companies
- Employment history (for example, to identify potentially close relationships between former colleagues who now represent supplier and customer)
- The nature of the relationship between the public entity being audited and particular suppliers (for example, to identify misuse of inside information for potential bid rigging)

To ensure that available resources are used on high risk cases, in-depth inquiries should be carried out *after* having completed introductory inquiries. Hence, in the beginning, the auditor should try to avoid 'digging too deep', and rather concentrate the efforts on *1) assessing the internal controls of the entity* and *2) identify cases which illustrate possible weaknesses in the internal controls*.

***Further inquiries pertaining to procurements - selection of invoice:***

Usually, in inquiries of selected transactions it will be sufficient to obtain one invoice per supplier. However, the selection of the invoice should not be at random, but be based on knowledge regarding which red flags are relevant for the entity being audited. The invoice will be of assistance to the auditor by providing additional information regarding the transaction/supplier which cannot be seen from the financial statements.

The following questions may be relevant for the further scrutiny of an invoice:

- *Specification* on the invoice. What goods/services are being delivered? Is the delivery sufficiently specified?
    - Among other things, the auditors should look for the name(s) of consultant(s), number of hours used, type of item delivered, work carried out, etc.
- To what extent can the invoice inform the auditor about the *background* for the transaction?
- Does the information provided on the invoice comply with the *requirements* in relevant *legislation*?
- How does the invoice appear?
    - The appearance of the invoice may give an impression of the 'professionalism' of the supplier
- Does the invoice contain references to persons, entities, orders and/or contracts?

***Report on red flags:***

The results from the analysis and the inquiries should be summarized in a red flag-report which usually is supposed to contain information on 50-80 transactions selected according to criteria such as the ones presented in the table above. Experience has shown that a minimum of 50 transactions often is necessary to gain sufficient insight into the entity in question, and that more than 80 transactions often are practically difficult to deal with. The red flag-report should ideally be made in a spreadsheet like Excel, as this makes it easy to edit, sort and colour rows and columns.

First and foremost, the red flag-report is a tool which is used to keep a general overview of potential risk areas, possible red flags and results from inquiries. The report should indicate which transactions/cases should/must be followed up, and which risk elements seem to be most apparent.

To avoid rash conclusions and unjustified accusations, it is important to maintain an objective and precise description of findings in the red flag-report. A red flag-report contains information on:

- Details from the accounts (regarding recipient, relevant department in the entity, voucher number and date, amount of the relevant payment and the total amount of payments in the period of study);
- The basis for the payment, such as an invoice;
- Payment patterns for the chosen period;
- Results from research in public registers;
- Other internal information from the entity (information regarding orders, contracts, routines, protocols, written correspondence, etc.);
- Results from more general research on the Internet;
- Prioritization in the audit:
    - **Red colour** indicates that the analysis has identified several red flags - thorough evaluation and extended inquries are given high priority;
    - **Orange colour** indicates that the analysis has identified red flags - evaluation and inquiries are given priority;
    - **Green colour** indicates lower priority and suggests that introductory inquiries do not indicate a need for further follow up.

As with risk assessment schemes, red flag-reports may also be 'living documents' which are supplemented and updated as new information is obtained. This ensures that the risk of fraud and corruption is approached in a systematic manner, and that accumulated knowledge on the internal controls of the entity is properly utilized.

***Overall summary of the transaction analysis:***

A proper presentation of findings motivates further follow up of important risk areas, and also facilitates dialogue on how individual findings should be dealt with in the further audit work. Hence, in the last phase of the transaction analysis an overall summary report should be made, which:

- Presents the overall purpose and scope of the analysis;
- Describes the analysis step by step (risks, data extracts, selection of transactions, inquiries, information sources);
- Repeats main observations and important risk areas;
- Provides examples (from the red flag-report) on the various risk areas;
- Provides recommendations on further work.

# Appendix E:
# **Confidential and sensitive interviews**[42]

Interviews are a common and useful method for collecting data and obtaining audit evidence for both financial, compliance and performance auditors, and they can also be of great use in cases concerning possible mismanagement, fraud and corruption. Due to their sensitive nature, however, it is advisable that auditors are particularly cautious when planning and conducting interviews in such cases.

Both in cases where someone is reporting on possible fraudulent and corrupt acts carried out by *others*, and in cases where the one being interviewed may be involved in fraudulent and corrupt acts *her-/himself*, the situation can be very challenging for both the interviewer and the interviewee. People in the first category, i.e. 'whistleblowers', may for instance experience a loyalty conflict between their duty to report on possible misconduct, on the one hand, and their considerations for the colleague(s) in question, on the other. Or they may be afraid of possible persecution, dismissal or other forms of retaliation if they tell what they know. And people in the second category may also very quickly begin to feel the pressure if the interview focuses on their personal involvement in possible fraud and corruption, mismanagement and other illicit or improper conduct.

This again can be very demanding for the interviewer, as the interviewee may show feelings and reactions which auditors normally do not experience in regular interviews. Moreover, confidential and sensitive interviews also may be difficult when it comes to obtaining the facts in the case, either because the interviewee tries to avoid answering the questions, or because she or he has an understanding and/or description of the facts which is biased. There may also be situations where the interviewee tries to take control over the interview or tries to manipulate the interviewer to reveal her/his own viewpoints and sympathies.

In general, confidential and sensitive interviews can be divided into planned and unplanned interviews:

**1. Planned interviews:**

This refers both to interviews with 'whistleblowers' and interviews with people who may be involved in fraudulent and corrupt acts themselves.

To start with, irrespective of type of interview, it is important to note that many SAIs enjoy the power of investigation. That is, their interviews with public employees or others receiving public funding do not necessarily have to be voluntary - the people in question can be required to appear for interview even though they rather would be let off. This gives public sector auditors a particular responsibility for acting professionally and for showing respect during interviews which can be difficult and/or unpleasant for the interviewee.

[42] Except from the last part on unplanned interviews, this appendix is mainly based on the following guideline produced by the Office of the Auditor General of Norway: "Veileder for etisk utfordrende intervjusituasjoner", June 2010.

***Before the interview:***

Before the interview, it is important to become well acquainted with the subject matter and to reflect on the purpose of the interview and the most central questions. In addition, if the interviewer is prepared for possible outbursts of feelings during an interview, she or he may be in a better position to deal with this in an appropriate manner if and when they occur.

As to the interviewee in particular, it is advisable to minimize as much as possible her or his possible uncertainty concerning the interview and the most central topics. This is done most appropriately by ensuring the highest degree of predictability for the interviewee before the interview starts:

- To the extent it is possible, contact with the interviewee should be established in due time before the interview. *Time and place* should be decided, and the *purpose* and the *main topics* of the interview should be communicated to the interviewee;

- Furthermore, the question of *participation* from both the SAI and the entity in question should also be clarified in due time. It is important to reflect on the *number of participants* in the interview. Experience has shown that there should be at least two participants from the SAI, among other things to maintain focus through the entire interview and as quality assurance, and not least because it can be very challenging to carry out this type of interviews alone. On the other hand, however, considerations for the interviewee suggest that the number of interviewers should be limited.

  Generally, the most important for the interviewer is to have the appropriate competence and sufficient knowledge regarding the subject matter. In some interviews, however, it may be advisable to bring a *leader/manager* from the SAI as support, if the interviewee also is a leader/manager. At the same time, one should be aware that the presence of leaders/managers from both sides may create a more formal atmosphere, which again may increase the risk that information is retained.

  In interviews where there is only one interviewee, it may be appropriate to allow her or him to bring an *advisor/counsellor*, as this may make her or him feel more comfortable during the interview. At the same time, however, it should be noted that the presence of such 'support persons' may affect the quality of the interview. Inter alia, this may be the case if the person in question is in a managerial position towards the interviewee, or if she or he is directly connected to the case in question and/or will be interviewed later in connection with this case.

- To the extent that this is something which can be controlled by the auditors, they should also consider carefully what type of *meeting room/facility* should be used for the interview. Large conference rooms and large physical distance between the interviewer and the interviewee(s) may also create a psychological distance between the parties, which again could make it more difficult to create trust and a constructive atmosphere for the interview.

- Also, it is important to *allocate sufficient time* for the interview, so that time is not a limiting factor if and when the interviewee provides information of a sensitive and confidential character. It is also advisable that this be communicated to the interviewee before the meeting.

***At the beginning of, and during the interview:***

At the beginning of the interview, the auditor should aim at giving the interviewee *a 'soft' start* and approach her or him in a manner which builds trust. This will make the interview appear less harmful and reduce possible power asymmetries. Such a 'soft' start can be established through a *well-prepared introduction* by the auditor. The introduction should inter alia briefly repeat the premises for the interview. In this connection, it also may be emphasized that the role of the auditor is not to be normative, but to describe the facts as objectively as possible. Moreover, if the interview is supposed to be verified by the interviewee, it is advisable that this also be communicated in the introduction, as this also may have a reassuring effect.

During the interview, it is very important that the interviewer *proceeds carefully*. If he or she appears too pushy, with too many direct and specific questions - especially at an early stage in the interview - there is a risk that the interviewee becomes more reserved, and tells less than she or he would have done if the interviewer had appeared less pushy. Moreover, interviewees under pressure also may start looking for 'traps' in the questions from the interviewer and try to avoid these, rather than reflect on the answers they give. Hence, it is important that the interviewers *remain calm* during the interview, also when discussing difficult questions or when the interviewee begins to show strong feelings or reactions.

To a large extent, the tips and advice concerning the conduct of confidential and sensitive interviews are equally relevant for interviews with 'whistleblowers' and interviews with people who may be involved in fraudulent and corrupt acts themselves. Notwithstanding this, however, some aspects may be more relevant for the former than the latter category - and vice versa. These aspects will be further elaborated below.

*Interviews with 'whistleblowers':*

The following can be particularly useful to keep in mind when interviewing 'whistleblowers':

- To utilize the time available as efficiently as possible, suggest for the interviewee that she or he before the interview thoroughly reflects on what he or she wishes to convey to the auditor. If the 'whistleblower' also can provide *documentation* which is relevant for the case, she or he should also be encouraged to bring this to the interview, as this can be very useful for the further follow-up of the case;

- At the beginning of the interview the 'whistleblower' should also be informed about the rules and procedures which apply for the interview in respect of *professional secrecy, confidentiality and anonymization*. This is very important to create the trustful relationship which is instrumental in obtaining good and relevant information. At the same time, however, it is also very important to be realistic and not promise the 'whistleblower' more than the auditor and the SAI are able to keep. It can be very unfortunate both for the interviewee and the interviewers if the former initially is promised anonymity or confidentiality which later is withdrawn;

  Depending on the country in question, the anonymity and confidentiality provided by the SAI may apply only as long as the case is dealt with by the SAI on its own. That is, from the moment a fraud and corruption case is reported to the police and comes under criminal investigation, the SAI in question may be required to hand over all their material

concerning the case to the investigation and prosecution authorities. The SAI in question may also be required to hand over all their material to the police or the court through a court order, or the auditor responsible for the relevant interview(s) in the case may be summoned as witness. Hence, in their communication with 'whistleblowers' it is very important that the auditors have good knowledge of the relevant laws, regulations and procedures which apply in their respective countries;

- To create and maintain and trustful and good atmosphere, it also may be tempting for the interviewer to show understanding and empathy for the viewpoints of the interviewee. If this goes too far, however, it entails the risk that the SAI in question later on will be criticized as being too biased in its work. Hence, in the interview, it is important for the interviewer to *maintain a good balance* between having *a trustworthy appearance*, on the one hand, and being *objective and neutral* on the other.

*Interviews with people who may be involved in fraudulent and corrupt acts themselves:*

The following can be particularly useful to keep in mind when interviewing people who may be involved in fraudulent and corrupt acts themselves:

- In cases of possible fraud and corruption, it is very important that auditors to the extent possible and as long as possible prevent suspicions from being thrown on individuals or within the entity in general. To avoid that the interviewee gets the feeling of being suspected or exposed, or that people in her or his working environment get this impression of the interviewee, it is advisable to carry out the interview *step by step* through several *exploratory talks*. With this approach it may be appropriate to have an *introductory round* with interviews or talks *with several actors*. In addition to the objective of *shielding the main possible 'suspect'* for as long as possible, this introductory round also serves the purpose of getting the best possible survey of the situation, including inter alia mapping the central actors and different aspects of the case.

- As already indicated, when turning to particular individuals, it may be advisable to start confidential and sensitive interviews 'softly' and proceed carefully. This is especially important when the interviewee may be involved in improper acts her-/himself. Hence, it is advisable to start with *open questions*, and *what*- and *how*-questions before turning to more *closed* questions, or asking *why*-questions. This implies that the interviewer first seeks to sort out the facts, for instance by starting with non-sensitive factual questions, before asking the interviewee for analysis and explanation.

  Even if the interviewer is well aware of the background for the subject matter, it can be a good 'investment' to start the interview with some *background-questions*. Furthermore, if and when the interviewee has started explaining matters, the interviewer should avoid interrupting too early, so that the interviewee can be allowed to *open up* in a pace that she or he is comfortable with.

- *Friendliness and respectful treatment* are important principles for all interviews, including interviews with people who may be involved in fraudulent and corrupt acts themselves. In practice, if the interviewee for instance shows clear signs of stress or anxiety, this may imply taking a break to give her or him time to recover or calm down, showing the interviewee that one understands that the subject matter is difficult to talk about, or temporarily change the subject with the possibility of returning to more sensitive issues

later in the interview. It is important to ask the interviewee whether or not she or he wishes to continue the interview when the interviewer sees that the former shows clear signs of strain.

- Generally, in cases of possible fraud and corruption auditors should *proceed very carefully*, so that they do not interfere with ongoing or potential future investigations and legal proceedings. (See, inter alia, paragraphs 4.7 in ISSAI 300, paragraph P21 in ISSAI 1240 and subchapter 7.4 in ISSAI 4200). Inter alia, it may be required for SAIs to contact the investigation and prosecution authorities when:

    - They have a confirmed suspicion that the case in question involves criminal offences;
    - This is believed to be necessary to prevent further fraudulent and corrupt acts from taking place;
    - There is a risk that evidence may be destructed;
    - There is reason to believe that the suspected will try to escape from investigation and/or criminal prosecution;
    - There seems to be a need for searching the suspect's residence, room or repository;
    - There seems to be a need for seizure of assets which the suspect have in her/his possession.

  Still, there may be situations where the police has not yet been involved and the interviewee during the interview with the auditors is about to admit that she or he has been involved in a criminal offence. In such situations, depending on the national legislation and the mandate of the SAI in question, the auditors may be required to caution the interviewee and inform her or him that she/he has no duty to give evidence which later can be used against her-/himself in a court of law, i.e. *self-incrimination*.[43]

  Hence, before conducting interviews where situations like this may arise, auditors should have good knowledge of their mandate and the relevant national legislation, consult appropriate legal and other counsel, and also thoroughly consider the *tactical implications* for their own inquiries as well as possible investigations by the police.

**2. Unplanned interviews[44]:**

This refers to interviews when individuals suddenly and unexpectedly approach the SAI in question, usually by phone, to report on possible misconduct, fraud and corruption in the public sector. Although such interviews cannot be planned in depth, they can still be prepared to some extent. Hence, below, some tips and advice that can be useful for auditors to keep in mind if and when they receive this type of phone calls will be presented.

*Before the phone call:*

The auditor should be mindful of the main objectives - from the SAIs perspective - for this type of phone calls:

- Receive and take note of relevant and material information;

[43] See also Jones, 2004, appendix 3, p. 190.
[44] This part is mainly based on another guideline produced by the Office of the Auditor General of Norway: "Telefonsamtale med tipser", August 2010.

- Endeavour to give the 'whistleblower' a feeling of being heard and understood;
- At the same time, explain the role and duties of the SAI for the 'whistleblower', so that she or he understands that she/he cannot expect the SAI to solve her/his 'case' and/or receive feedback on the further processing of the information given.

*When receiving a call:*

The auditor should ask for and repeat the name of the caller. If it is a regular name, the auditor also may ask where she or he is calling from. Furthermore, the auditor should ask for the phone number or note it down if it shows on the phone display. The auditor should then present her-/himself and explain her/his role - and take control of the conversation. At the same time, the auditor should endeavour to stay calm - this should not be a 'rush job'.

If required, the auditor should also explain the role and duties of the SAI, and inform about the rules and procedures which apply in respect of professional secrecy, confidentiality and anonymization.

Lastly, the auditor should also inquire whether the caller also has contacted other actors regarding the subject matter.

Then the auditor should allow the caller to tell her or his story, without interrupting too early, so that the latter can be allowed to explain the subject matter in a pace that she or he is comfortable with. In this phase, the auditor should mainly note down key words. However, the auditor may intervene if:

- the story is difficult to comprehend (too detailed, too incoherent, no 'story line', too implicit);
- the information is not relevant for the SAI;
- there is something that the caller probably has misunderstood.

Eventually, it will be necessary to summarize the tip and this should be done together with the caller. The auditor should not be afraid to ask again about important matters - what are the most central elements of the tip?

- Does the tip really concern possible fraud and corruption? In this regard, the auditor should try to focus on:
    - *What* is happening/has happened?
    - *Who* are involved/behind?
    - *How* are the fraudulent and corrupt acts carried out?
    - *When* did this happen or is it happening in the present?

- Furthermore, the auditor should ask the caller what the information is based on (own observations, observations by others, assumptions based on observations, etc.)

- The auditor may also consider asking the caller if she/he could make a written résumé and send this to the SAI, and - if possible - enclose relevant documentation.

*At the end of the call:*

The ending of the call is important. A good ending is important for the caller to feel comfortable and satisfied with the response, and not expecting any further feedback, as long as the auditor does not indicate that she or he wishes to have a follow-up talk at a later stage.

It is also important to thank the caller for providing the tip, and emphasizing that tips from the public are an important source of information for the SAI.

*Important to remember:*

- As with planned interviews, the auditor should not promise the caller more than she or he can keep - whether this concerns the aspect of confidentiality and anonymity or the further follow-up of the case - and also endeavour to maintain a balance between having sympathy for the caller, on the one hand, and remaining neutral and objective as to the facts of the case on the other.

- It is advisable to keep this list of tips and advice, as well as brief texts on the role of the SAI and the general procedures for the further processing of tips from the public within reach, so that these are easy accessible if and when the phone rings.

# Appendix F:
# **Procedures for receiving and handling confidential and sensitive information**

The establishment of a confidential 'hotline' where both employees and people outside the government agency in question can provide tips on possible fraud, corruption and other kinds of misconduct can be a very effective reporting mechanism.[45] In other words, it can be a very effective tool to *detect* fraud and corruption. In addition, however, it can also be a very effective *prevention* mechanism as the mere existence of and reference to such a hotline can give employees a perception of high probability of detection, thereby being a strong deterrent. Moreover, by establishing and promoting a fraud and corruption 'hotline', i.e. by allowing employees and others to report misconduct without fear of retaliation, the organization will also send the message that it is sincere in its efforts to create an environment of ethics and integrity.[46]

*Confidentiality* is – as already indicated – a fundamental prerequisite in this regard. That is, the reporting mechanism should be constructed in such a way that employees and others are allowed to report or seek advice anonymously or confidentially regarding actual or potential misconduct by others within or outside the government agency or entity in question. Furthermore, the anonymity and confidentiality should also be clearly emphasized in all communications regarding this mechanism, so that 'whistleblowers' can be assured that their reports and their identity will be kept confidential.

Also, in addition to the technical arrangements, it is important that the organization in question has a 'whistleblower' policy in place which makes it clear that employees and others reporting misconduct do not have to fear retaliation under any circumstance as they will receive the necessary protection. Just as critical as confidentiality, however, is to ensure that hotlines are not abused, that is, to protect the rights and reputations of individuals against false allegations. Both prerequisites – i.e. confidentiality and protection against abuse – necessitate inter alia proper procedures for dealing with tips and competent and experienced interviewers.[47]

As an example on how this can be arranged in practice for SAIs wishing to receive external tips on possible fraud, corruption and other kinds of misconduct in the public sector, the procedures of the Auditor General of Norway for receiving and handling confidential and sensitive information - including a confidential 'hotline' - are further described below.

[45] According to the 2010 Global Fraud Study, carried out by ACFE, tips were by far the most effective detection method in the period of study (2008-2009), as they resulted in the detection of almost three times as many fraud cases as any other method. This is also consistent with the findings in ACFE's previous studies. Moreover, the 2010 study also showed that there was a correlation between the presence of fraud hotlines and an increase in the number of cases detected by a tip. Source: ACFE, 2010. Report to the Nations on Occupational Fraud and Abuse. 2010 Global Fraud Study. [Online] Available at www.acfe.com/rttn/rttn-2010.pdf [Accessed on 30 March 2011], pp. 16-17.

[46] ACFE, 2006, pp. 8-9; Dye, 2007, pp. 318-319.

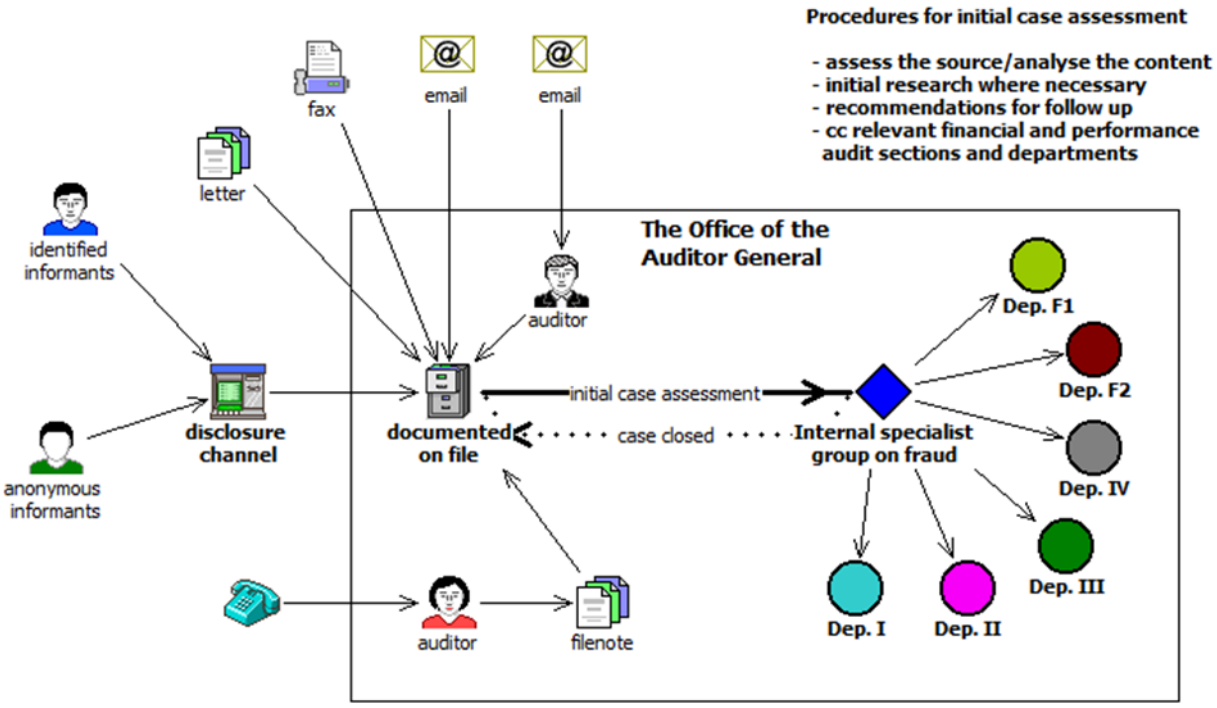
[47] ACFE, 2006, p. 9; Dye, 2007, p. 319.

## THE PROCEDURES OF THE AUDITOR GENERAL OF NORWAY FOR RECEIVING AND HANDLING CONFIDENTIAL AND SENSITIVE INFORMATION FROM THE PUBLIC:

In 2008, as part of its efforts to prevent and detect fraud and corruption and other kinds of misconduct in the public sector, the Office of the Auditor General (OAG) established a confidential disclosure channel and adopted procedures for handling confidential and sensitive information from the public.

In addition to tips received through the disclosure channel, the OAG also receives information from the public through e-mails, letters, faxes and telephone. All tips are documented on file in the central record office of the OAG, before they are forwarded to the Internal Specialist Group on Fraud (ISGF), which also was established in 2008. The ISGF is responsible for the initial case assessment, before the case is further distributed to the relevant sections and departments in the OAG. This is illustrated in figure G.1.

**Figure G.1: The procedures of the Office of the Auditor General of Norway for receiving information from the public and for initial case assessment**




The purpose of the initial case assessment in the ISGF is to ensure that all tips and cases are dealt with uniformly and professionally from the time of receipt. Furthermore, this also provides the OAG with even stronger assurance that relevant and concrete information on possible fraud and corruption is properly utilized in the regular audit work.

All tips are, as a minimum, assessed by two members of the ISGF. If the initial assessment suggests that the tip concerns possible fraud and corruption, the case is subject to further quality assurance before it is forwarded to the relevant section in the OAG. The assessments of the ISGF are always summarized in a separate note which is enclosed with the other documents of the case.

All tips and notes from the ISGF are forwarded to the responsible section, both within the financial and performance auditing branches of the OAG. This provides for greater awareness of tips concerning possible fraud and corruption, as well as better learning in the organization. The initial case assessment in the ISGF also provides for competence building among the members of this group.

At the same time, however, confidentiality is a fundamental premise for the handling of, and the communication regarding all tips in the OAG.

Usually, the initial case assessment in the OAG consists of three steps: a) An assessment of the source ('whistleblower') who has provided the tip/confidential information; b) An assessment of the actual content of the tip; c) A recommendation on *whether*, and if so, *how* the tip could/should be followed up.

***a) Assessment of the source:***

The purpose of this assessment is to get an idea of how reliable the information in the tip appears to be, and whether the information given also can be verified through independent sources. In this connection, possible motives of self-interest behind the tip, or whether the tip appears to be biased, are also considered. If the source/'whistleblower' is anonymous, however, the ISGF can only assess her or his trustworthiness on the basis of an assessment of the reasonableness of the content of the tip.

If the source is not anonymous, the ISGF also may recommend further contacts with her or him, if this is considered to be beneficial for the further processing of the case.

***b) Assessment of the content of the tip:***

In its assessment, the ISGF provides a short summary of the main elements of the tip, and puts emphasis on the core of the problem described by the source. Emphasis is also laid on whether, and if so, how the tip is documented, whether there are references to further information in the case, and whether the information can be verified through publically accessible sources and/or relevant registers which are accessible to the OAG. All information gathering carried out by the ISGF are summarized in the note, and relevant documentation from this research is also enclosed.

***c) Recommendation on whether and how to follow up:***

On the basis of the assessment of the source and the analysis of the content of the tip, the ISGF gives a recommendation to the relevant section and department in the OAG. The recommendations can be divided into the following three categories:

(i) The case should be followed up and subject to further information gathering. In such cases the ISGF also requests the relevant section to report back on the results from these further inquiries. Normally, the ISGF also offers to provide methodological support to the section/department in question if this is required;

(ii) The information provided in the tip does not concern possible fraud and corruption, but is still considered to be useful as background material for the regular auditing work of the section/department in question;

(iii) The tip is not considered to be relevant for the OAG. The case is then closed by the ISGF.

Both in cases where the OAG have suspicions of possible fraud and corruption, and in cases where fraudulent and corrupt acts actually can be demonstrated, the OAG never concludes on whether fraud and corruption also has taken place in a *legal* sense, as this must be confirmed by a court of law. In instances where the OAG has suspicions on serious criminal offences, it may be most appropriate to forward the case directly to the investigation and prosecution authorities. Usually, however, it is left to the audited entity to decide on whether or not to report the matter to the police.

# Appendix G:
# **Audit evidence, documentation and reporting**

The audit steps and procedures which apply more generally to the gathering of audit evidence, documentation and reporting are equally important in cases concerning possible mismanagement, fraud and corruption. Below, these three stages in the audit process will be briefly described with a particular focus on fraud and corruption risks.

### Audit Evidence:

According to ISSAI 300, paragraph 5.1, "[c]ompetent, relevant and reasonable evidence should be obtained to support the auditor's judgement and conclusions regarding the organization, program, activity or function under audit".

The specific audit procedures to be performed will however depend on the professional judgement of the auditor, as well as the identified criteria and the particular features of the subject matter. The procedures should also clearly reflect the risks identified and be carefully chosen.[48] In cases of possible fraud and corruption auditors should be particularly careful when gathering evidence, so that they do not interfere with ongoing or potential future investigations and legal proceedings.[49]

According to ISSAI 4200, techniques for gathering audit evidence may inter alia involve the following[50]:

1. *Observation,* i.e. watching or observing a procedure or process when it is being performed.

2. *Inspection,* i.e. examining accounts, records and other case documents or tangible assets.

3. *Inquiry,* i.e. requesting information from persons who are considered relevant, both within and outside the public sector entity in question. Inquiries may vary from informal talks to formal written communications. Interviews of relevant persons, including experts, may also be part of such inquiries. (See also appendix E).

4. *Confirmation* (also a type of inquiry), i.e. requesting replies directly from third parties concerning particular matters, without involving the audited entity.

5. *Re-performance,* i.e. independently performing the same procedures as already have been carried out by the audited entity. Re-performance can be carried out manually or through computer-assisted audit techniques.

6. *Analytical procedures,* which include comparing data, or studying variations or relationships which seem to be inconsistent.

[48] ISSAI 4200, paragraph 96; ISSAI 300, paragraph 5.2.
[49] See, inter alia, paragraphs 4.7 in ISSAI 300, paragraph P21 in ISSAI 1240 and subchapter 7.4 in ISSAI 4200.
[50] These techniques are further elaborated in paragraphs 106-117 of ISSAI 4200. As to audits of financial statements in particular, supplementary guidance is also provided for in ISSAI 1500.

As a general rule, it is advisable to get *verbal facts and opinions* confirmed in writing, if possible. Such confirmations may inter alia relate to: Balance owed; instructions sent out; warnings issued; work taken on; dates and times, etc. In addition, although they may seem trivial at the time they emerge, it can be useful also to document other verbal facts being given during the ordinary course of events, as these may turn out to be more significant at later stages. To prevent possible suspicions from being known among individuals or within the entity in general, however, such inquiries may need to be done carefully and discretely.[51]

When possible and relevant, *photographs* may also provide valuable evidence. In that case, it may be advisable to use cameras which have a built-in time display.[52]

## Documentation:

According to ISSAI 300, audit evidence must be adequately documented. The documentation should include the basis for and the scope of the planning, work carried out and the findings of the audit. The documentation should be sufficiently detailed and complete to enable experienced auditors with no prior knowledge of the audit to understand what work has been carried out to support the conclusions. (Paragraphs 5.5 and 5.7).

### *Structuring and systematization of documentation[53]:*

It is important for auditors to get their records and evidence properly organized. In many inquiries, this is often among the weak points and therefore it usually merits special attention. Moreover, it is also advisable that the routines and practices for structuring and systematizing audit evidence are as uniform as possible.

Among other things, it is advisable that auditors:

- Retain all relevant documents, hard copy printouts, etc. When it comes to documents from various registers containing information regarding particular organizations and/or persons, it may often be advisable to print out these documents instead of storing them electronically. This both due to sensitivity aspects (see below), but also because it will make it easier to juxtapose and analyze data gathered from different sources;
- Initial or password-protect and date all documents. As to original documents in particular, it may be critical to ensure that these are dated and even timed. Auditors should also ensure that the sources of evidence always are clearly stated, also when this is an anonymous informant;
- Update and cross-reference all their audit evidence and working papers. It is advisable that the evidence and associated working papers have a quality and a format which make them understandable also for non-auditors, such as a police officer;
- Provide all their papers with a file and page reference, and have them listed in a file index;
- Ensure that all cross-references in the documents are easy to notice;
- Depending on the volume of documents, organize them in binders.

[51] Jones, 2004, appendix 3, p. 189.
[52] Jones, 2004, appendix 3, p. 190.
[53] This part is based on "Veiledning i bruk av transaksjonsanalyse til vurdering av risiko for misligheter", December 2011, and Jones, 2004, appendix 3, pp. 189-90.

***Storage, safe-keeping and deletion of sensitive data[54]:***

On the one hand, it is important that all auditors involved have easy access to all files and documents pertaining to the case in question. At the same time, however, in cases of possible fraud and corruption, there may be documents among the evidence gathered which contain sensitive information about individuals or other matters. Auditors should therefore pay attention to data protection of such information, and also be aware that the use and storage of sensitive and personal information may be subject to particular requirements under national legislation. (See also appendix C).

In practice, it may be under the discretion of the auditor or his or her leader to find the proper balance between accessibility, on the one hand, and protection of the privacy of individuals or other confidential information on the other. Depending on national legislation, however, it may under any circumstance be required to delete/destruct all documents and files containing personal information when such data no longer are necessary for the inquiry in question.

## Reporting:

In cases of possible fraud and corruption, SAIs may be required to report such matters to appropriate levels of management within the audited entity, to those charged with governance (i.e. ministerial or administrative bodies higher up in the reporting hierarchy), to the legislature, or to the relevant law enforcement authorities. The specific requirements for such reporting may vary, however, depending on the mandate of the SAI and national legislation.[55] (See also appendix E).

As to the public reports from SAIs, i.e. the reports to the legislative or another responsible public body, anonymization of individuals is often the rule. Due to privacy considerations, protection of whistleblowers, etc. such anonymization may become even more important in cases of possible fraud and corruption. In some cases, however, full anonymization can be difficult to achieve. This may for instance be the case where there are references in the report to a specific position or title within the audited entity which there is/are only one or a very few of. Hence, in those instances where information in the report easily can be traced back to individuals, it may be advisable to consider the publicizing of such information carefully.[56]

In addition, there may also be circumstances where the publicizing of specific information regarding fraud and corruption in the public sector may compromise ongoing investigations or legal actions. In such cases, it is important that SAIs consult with other relevant authorities, such as law enforcement agencies, to decide what can be publicized or not.[57]

[54] Where not otherwise stated , this part is based on the following guideline produced by the Office of the Auditor General of Norway: "Saksbehandlingsregler - opplysninger om enkeltpersoner i mislighetssaker", 3 March 2011.
[55] ISSAI 1240, paragraphs P20 and P21; ISSAI 4200, paragraphs 126 and 130.
[56] "Saksbehandlingsregler - opplysninger om enkeltpersoner i mislighetssaker", OAG, 3 March 2011; "Veileder for etisk utfordrende intervjusituasjoner", OAG, June 2010.
[57] Dye, 2007, p. 320; UNODC, 2004, p. 105. See also ISSAI 1, Section 16.3.