



14th meeting of the INTOSAI Sanding Committee on IT Audit
Bhutan, 27 – 29 April 2005

AGENDA ITEM 3C

Scoping paper possible fraud project

13 April 2005

1 Introduction

This project has its origin in an NAO survey on IT-related fraud. One of the results of the survey showed that it was not possible or hard to make a clear distinction between 'ordinary' and 'computer-related' fraud. To give a simple example: if someone used the phone to order some merchandise using a stolen credit card, we may consider this fraud. However, when they place the same order via a website, aspects of IT or computer-related fraud may be triggered. Finally, many of the measures meant to mitigate risks that were mentioned by the respondents proved to be general fraud combating measures, and not specifically aimed at computer-related fraud.

In order to better understand the distinction, the Netherlands Court of Audit offered to try to integrate the IT aspect into the fraud survey we were doing at the time. However, it became clear that the specificity of this aspect did not mix well with the more general level of the other aspects in the project.

Therefore, during the 13th meeting held in Moscow in 2004, we pleaded for more time to be able to outline a new route. The meeting decided that we were to produce a scoping paper, which is in front of you now.

2 Fraud

2.1 Relevance

Fraud is of interest to SAIs because it presents governments with substantial financial losses and/or loss of credibility (specifically in the area of the integrity and incorruptibility aspects of good governance).

2.2 Terminology

Fraud is an umbrella term used to refer to various types of deliberate improper behaviour, resulting in some unfair or dishonest advantage for one party and a corresponding financial loss and/or loss of image for another party. These



behaviours can be categorized as irregularities, wrongdoing and fraud (see appendix 1). Here we will use the umbrella term 'fraud' for convenience.

2/6

2.3 *Locale*

- Internal: fraud within the organization.
- Vertical: fraud by external parties (suppliers, customers, citizens) to the detriment of government.
- Horizontal: fraud where one external party (an individual or a business) harms the other.

2.4 *Phases in combating fraud:*

- Prevention.
- Detection.
- (Criminal) investigation.

3 Scoping

Irregularities, wrongdoing and fraud – fraud for short – are all relevant. Because our primary interest is losses that government may suffer, we can leave horizontal fraud aside. Hence the fraud locales that we need to take into consideration are Internal and Vertical.

4 General approach

Given that a SAI's mandate typically does not specify (criminal) investigation powers, the phases of interest to us are Prevention and Detection. When speaking about the prevention and detection of fraud we are essentially talking about internal controls. INTOSAI's recent renewal of its set of guidelines on internal controls provides us with a good set of criteria in this regard¹ (see Appendix 2). The guidelines have a clear bearing on the fight against fraud and also hint at some major IT aspects. They need however further specification, as regards both the fraud element and the IT aspect. We can use existing approaches for this purpose.

Regarding the fraud element we are aware of a number of frameworks that are relevant. We could either choose one or assemble a new one, custom-made for our purpose with components from existing frameworks.

In the IT area we can for instance draw on the INTOSAI IT Audit training materials, on CobiT² and on IFAC standards³.

¹ Guidelines for Internal Control Standards for the Public Sector.

² <http://www.isaca.org/>. A (free) registration is required to gain access to the CobiT framework.

³ <http://www.ifac.org/>.



5 Proposal

We propose to mount a project aimed at building a framework for the audit of fraud combat along the lines of the approach described above. It is aimed at combating fraud as an essential component of good governance in the public sector. The framework will list and explain in general terms:

3/6

- (1) how the auditee may utilize IT to build controls for the prevention and detection of fraud,
- (2) which minimum set of measures the auditee should have in place to safeguard its IT infrastructure and fraud-sensitive information systems against possible fraud-oriented attacks from inside or outside the organization,
- (3) how SAIs can audit the items (1) and (2) above,
- (4) how SAIs can use automated tools to analyze financial data and logging data in search of possible fraud cases (including tools for the generation of 'red flags', i.e. indicators of high fraud-risk situations).



Appendix 1: Definitions of irregularities, wrongdoing and fraud

Source: training CD-ROM 'Irregularities, Wrongdoing and Fraud' produced by the INTOSAI Development Initiative (IDI)⁴.

4/6

Irregularities

Irregularities refer to intentional misstatements or omissions in the accounting records or financial statements for whatever purpose, and/or a misappropriation of the entity's assets, whether or not accompanied by misstatements of accounting records or financial statements.

Wrongdoing

The term wrongdoing refers to intentional inappropriate activities such as conflict of interest, gross administrative abuse, misuse of funds or assets, theft, abusing, exceeding or non-compliant with authorities and unethical behaviour, and may include irregularities.

Fraud

Fraud is a term that embraces all the means that human ingenuity can devise, which is used by one or more individuals to get an advantage over another by false representations. More than one legal definition of fraud exists.

For the purpose of this course fraud is referred to as a deliberate act that usually involves the use of deception to obtain some form of financial benefit or advantage from a position of authority or trust, which often results in some form of loss to the organisation being defrauded. Fraud can include serious irregularities, wrongdoing, dishonest acts, deceit, illegal acts such as false representation, fraudulent concealment, theft, secret commissions, kickbacks, breach of trust, collusive bidding and other illegal activities of a similar nature.

Fraud can only be confirmed and determined by a court of law. Auditors can only determine that matters appear or are suspected of being fraudulent.

Fraud may involve:

- Falsification or alteration of accounting records or other documents
- Misappropriation of assets or funds including theft
- Suppression or omission of the effects of transactions from records or documents
- Recording of a transaction without substantiating documentation
- Intentional misapplication of accounting policies
- Wilful misrepresentations of transactions or of the entity's state of affairs

⁴ The training arm of INTOSAI.



Appendix 2: INTOSAI Guidelines for Internal Control Standards for the Public Sector.

5/6

Definition of internal control

The INTOSAI guidelines define Internal Control as follows:

Internal control is an integral process that is effected by an entity's management and personnel and is designed to address risks and to provide reasonable assurance that in pursuit of the entity's mission, the following general objectives are being achieved:

- *executing orderly, ethical, economical, efficient and effective operations;*
- *fulfilling accountability obligations;*
- *complying with applicable laws and regulations;*
- *safeguarding resources against loss, misuse and damage due to waste, abuse, mismanagement, errors, fraud and irregularities.*

Particularly the last bullet in the list makes it clear that internal control is pivotal to fraud combating.

Components of internal control

The guidelines are structured along the lines of the COSO framework⁵, which recognizes the following five components of internal control:

- Control Environment
- Risk Assessment
- Control Activities
- Information And Communication
- Monitoring

Especially the components *Control Environment* and *Control Activities* are of interest to us.

Control Environment

The control environment is the foundation for the entire internal control system. It provides the discipline and structure as well as the climate which influences the overall quality of internal control. It has overall influences on how strategy and objectives are established, and control activities are structured.

Control Activities

The guidelines prevent the following examples of *control activities*:

- authorization and approval procedures;
- segregation of duties (authorizing, processing, recording, reviewing);
- controls over access to resources and records;

⁵ http://www.coso.org/publications/executive_summary_integrated_framework.htm.



- verifications;
- reconciliations;
- reviews of operating performance;
- reviews of operations, processes and activities;
- supervision (assigning, reviewing and approving, guidance and training).

The reader will easily recognize the relevance of IT in this context. Not surprisingly, a separate section is devoted to IT control activities, according to the well-known division of IT controls into general controls and application controls.