

# **The Disclosure and disposal of fraud in IT environment**

## **China National Audit Office**

As a team member of the project of “Anti-fraud in IT Environment“, the CNAO pays much attention and commits itself to disclose the IT-related fraud. Although there is still some development gap in the IT field between China and the developed countries, we also have to face some troubles from IT-related fraud. Based on our own experiences in this field, the CNAO has submitted two country papers successively at the 15<sup>th</sup> and 16<sup>th</sup> Committee meeting, they are: “Characteristics of the fraud in IT environment” and “Measures Taken to Counter Fraud in IT Environment”. As one part of the series, the CNAO would like to share the idea about the “Disclosure and disposal of fraud in IT environment” at this meeting.

### **1. Special considerations on the disclosure of fraud in IT environment.**

In the traditional financial audit, fraud refers to the deliberate activities which would result in untruthful reflection of financial statements. From the beginning, IT Audit committee defines fraud in IT environment as follows: in order to get the dishonest benefits or harm others’ interests, the organization or the personnel undertakes secret IT-related activities. In view of this, our research on fraud moves beyond the traditional scope of financial statements and covers all possible illegal secret activities. In the meanwhile, we try to focus our efforts on the IT-related fraud. It can be said that the research on fraud in IT

environment is a specific issue. Compared to fraud in traditional financial auditing, there are four special considerations when we disclose the fraud in IT environment.

1.1 Consideration based on the diversity of subjects who make fraud in IT environment. In the traditional auditing environment, fraud usually occurs from inside the audited entity. For instance, the management commits deliberate top-down frauds by inventing or even hiding the facts; some of the staff forge, modify or even destroy relevant records to search for personal benefits. While in IT environment, fraud always comes from the outside, for instance, the hacker breaks in the system and modifies the data through Internet. Actually such fraud is against the interests of the audited entity. While the management should take the responsibility for the weakness, they are also the victim to a large extent. Under such circumstance, auditor should differentiate respective responsibilities based on special consideration before disclosure.

1.2 The disclosure covers beyond the untruthful reflection of financial statements. In contrast with the traditional auditing, auditing scope and the contents have greatly changed in IT environment. More and more auditing work is beyond the check of accounting books, especially for government audit institutions. As a result, the fraud detected also surpasses accounting materials and affects more than the authenticity of financial statements, thus in the same way audit risk is not only limited to the judgment about the authenticity of financial statements. For instance, if the audited entity colludes with IT companies to develop accounting software which are used for fraud, this is completely different from the fraud arising from

manual adjustment of accounting records in financial statements. When making the disclosure, the auditor should also take such collusion between audited entity and IT companies – which is more serious – into account. Audit institution should make special consideration on the scope and the contents of IT-related fraud.

1.3 Before the disclosure and disposal, audit institution should consult more with external specialists. The IT-related fraud-makers are usually very familiar with business procedure and make a lot of research on IT, and apply much professional expertise on computer, database, network and so on. Auditors could not deem any advantage all the time even when they detect something during the gamble of identifying and confirming fraud. In order to ensure the accuracy of disclosure and reduce audit risks, auditors should be cautious enough and consult more with external specialists. According to the CNAO's experience, auditors usually work to determine the nature of IT-related fraud and disclose them much harder than in traditional financial auditing. Therefore audit institution should give special considerations to timing arrangements, human resource, cost relating to external specialists, and so on.

1.4 There should be some distinction of notification to the public among the frauds of different nature. As for traditional auditing, the fraud that would affect the authenticity of financial statements generally should be disclosed to the public to the largest extent. In such a way, investors and other stakeholders can understand facts and take corresponding measures to reduce the loss; it can also be conducive to punishments from moral, civil, administrative, and criminal aspects on the fraud-maker. In

most cases, such principles also apply for the disclosure of IT-related fraud. Just because of such unique characteristics as the diversity of subjects, good concealment, high intelligence, the difficulty of prevention, the differentiation should be made according to diverse scenarios before the disclosure of IT-related fraud. For instance, because of system weaknesses or equipment problems in telecommunication, some people could get the benefits from the information which he should not have obtained, or data are manipulated and destroyed due to ineffective and incomplete transmission. These are obvious IT-related frauds. However, if the disclosure is made before audited entity makes all-around improvements, it is actually nothing less than an act of advertisement and would probably expand the loss of audited entity and the effects of fraud. We notice that some SAIs pay much attention to it. Although they have made great achievements on detection of IT-related fraud, we can just find a few words in their audit reports on the Internet, and no any details about the weakness. Such experiences can be shared among us.

## **2. The form and contents of disclosure to different recipients**

Some people insist that all frauds, including IT-related fraud, should only be determined and affirmed by the law court. However, many audit institutions believe that auditors are capable of detecting possible frauds with due care by conducting proper audit procedures. In Oct 2002, after summarizing the suggestions from both research and practice, AICPA promulgated SAS No.99 *“Considering the fraud in financial*

*reports*”, replacing previous SAS No.82 “*Anti-fraud Auditing Standards*”, with an aim to enhance the capability of CPA to detect and disclose the fraud in the listed companies during the conduct of financial auditing. Early in 1996, CICPA, the Chinese Institute of Certified Public Accountants, issued “*Independent Auditing Professional Standard No.8 ---- Errors and Fraud*”. *Audit law* of P.R.China stipulates that audit institution “shall, according to law, supervise through auditing the authenticity, lawfulness and efficiency of the government or financial revenues and expenditures audit and supervise the reality, effectiveness and efficiency of the financial revenues and expenditures” and are entitled to detect fraud. Obviously fraud is neither a real nor a legal action.

It is the responsibility of audit institution to detect and correct errors, and disclosure is the important representation for audit organization to fulfill its supervision. Article 36 of Chinese *Audit Law* stipulates that “audit institutions may issue circulars about their audit results to the relevant government departments or publish such results to the public”. IT-related fraud, which was detected and confirmed by auditors, should be disclosed in audit report or in other proper form. The form and the contents should be different according to various recipients.

2.1 The disclosure to the public. Generally the disclosure is made by audit institution to the public by publishing audit reports, while CNAO takes the form of “Announcement of audit findings”. At present, in view of the feature of high concealment, the disclosure to the public is conducive to publicizing the forms and the consequences of IT-related fraud and expanding public awareness. The disclosure should focus more on the results and

harm instead of fraud details, just as the users should be aware of the existence of hackers and Trojan horse over the Internet for better prevention while the detailed techniques, such as hacker attacking, embedment of Trojan horse, etc, should not be elaborated to avoid unintentional advertisement.

2.2 The disclosure to the management. CPA will usually inform the management of fraud detected during the audit in a proper way, and ask the audited entity for proper disposal or disclosure in financial reports. Audit institution thinks it significant to notify the management about those IT-related frauds. Compared with traditional fraud, IT-related fraud is the integrated results of concealment, intelligence and diversity of fraud subjects. It is also a great challenge to the management. Unless the management is involved in the fraud, they would welcome the recommendations from audit institution on improving its management and remedying the weakness. While notifying the fraud to the management, audit institution should study together with the audited entity on how to build a better control system in IT environment, how to prevent and detect the fraud, what minimum measures taken to safeguard its IT structure and sensitive information, and how to defend the attacks from both inside and outside.

2.3 The disclosure to the authority. For audit institution, the management might not be the only recipient of audit reports, which is different from CPAs. Due to his limited power, a CPA can just issue qualified audit opinion or refusal if he suspects the management of fraud or the management refuses to make the adjustments or proper disclosure. Based on the *Accounting and Auditing Enforcement Release for 1987-1997* promulgated by

American Securities Exchange Committee (SEC), a survey on fraud cases in the listed companies showed that 72% of cases were involved with CEO and 43% with CFO, altogether 83% concerned CEO or CFO. It is the responsibility and power of audit institution to report to the authority if the top management is found to commit fraud or collude with others. In some countries, audit institution fulfills its responsibility by reporting the fraud to the parliament. Sometimes even the fraud is detected in audited enterprise, audit institution should report to its supervising authority for timely solution. Recently a case of fraud in Societe Generale in France led to the lose of 4.9 billion Euros, where the IT genius Jerome Kerviel forged relevant documents and broke through 5 passes into data system, and obtained the authority of using substantive amounts of fund. Such illegal action remained unnoticed for almost one year. If this typical IT-related fraud had been identified by audit institution and timely reported to the banking supervising body such as Bank De France or AMF, the results would definitely be opposite.

### **3. CNAO's investigation and disposal of IT-related fraud**

Although almost each audit institution has the power to both investigate and report, only a few SAIs can go further and focus on accountability and rectification. According to Chinese *Audit Law*, “where violations of State regulations governing government and financial revenues and expenditures should be dealt with and punished in accordance with law”, audit institution shall, “within the limits of its statutory functions and

powers, make an audit decision or put forward to department in charge its suggestions as to how to deal with or punish the violations.”

In recent years, with an aim of adapting to rapid development of national economy and IT management, the CNAO has strengthened IT training for auditors and improved its capability of audit and supervision in IT environment. Consequently many IT-related frauds have been detected in those organizations which have a wide application of information technology, such as monetary units, social securities and large-scale state-owned enterprises. That is also part of well-known “Audit Storm”. It should be noted that neither financial audit nor performance audit by the CNAO is deliberately aiming at IT-related fraud; however, the possibility of detecting these frauds would be greatly increased if auditors are equipped with appropriate competence with due attention, let alone the special audits with an aim to confirm IT-related frauds and those focusing on information system of audited entity. In China, there are two ways to deal with IT-related fraud by audit institution. One is to make the disposal by audit institution within the limits of its statutory functions, such as confiscating illegal gains and/or demanding the refund of money back to its original pool, etc; the other is to put the case forward to related departments, including transferring the case of government staff to the supervising departments for further investigation or suspicious cases to the judiciary organs.

In contrast with the punishment to the responsible person of IT-related fraud, the CNAO would rather attach more significance to rectification. Just as an old Chinese saying tells

“Never too old to learn, never too late to turn” , the most important thing of rectification is to identify the weakness and remedy it to improve the system. It could also be useful for people to learn about the form and consequence of IT-related fraud in order for better prevention. Now the general practice has already been shaped that measures taken by audited entity are described in the *Announcement of Audit Findings*, and it works well.

IT is changing our life. We should agree that IT does bring us civilized enjoyment much more than the troubles arising from IT-related fraud. As our audit cause goes further with time moves on, we are looking forward to more cooperation with other SAIs in this field of anti-fraud.