

**Measures Taken to Counter Fraud in IT Environment –
Based on Audit Practice in China
China National Audit Office**

Good morning Mr. Chairman and colleagues,

In Last year's ISCITA meeting held in Brasilia, the Chinese delegation made a presentation named "Characteristics of Fraud in IT Environment ". Further to the previous one today we will brief you on some initial results of our research on the topic of "Measures Taken to Counter Fraud in IT Environment " Our research is made on the basis of audit practice in China. In our audit work we found quite some fraud activities happened due to poor internal control. In our audit reports we put forward recommendations to improve internal control to prevent fraud activities. To improve internal control we need to strengthen control from the following five perspectives:

1.Organizational and personnel controls

IT fraud needs IT environment. The organization and personnel are the important factors.

- **Access control of software and hardware.** Whether the hardware is purchased or the software is upgraded, the access to the software and the hardware must be controlled in case of any risk.
- **Control of the positions of system management and maintenance personnel.** According to the incompatible principle, some positions should be separated, such as system administrator, software maintenance and management, hardware maintenance and management, etc. the operation role should be clear in order to avoid the illegality by the unauthorized people.
- **Control of business software users** even within the same section, such as the position of input, check, processing and output.
- **Control of archives.** Because it is easy to modify the data, it is necessary to backup the e-data timely in case of the check. These controls shall be the part of the disaster recovery.
- **Internal Audit.** The internal audit department should be separated from the management and responsible for the Board of directors. The capability, program and the mechanism should meet the related requirements of the internal audit work.
- **Personnel management.** It is necessary to make the personnel management to avoid IT fraud, such as recruit, the role description, vacation, independent check, demission, etc.

2.Data management

IT fraud is a kind of illegal activities that gets benefit by using IT. Usually it is related directly with data. So it is very important to prevent IT fraud by managing and controlling data. There are three control points:

- **Data input management.** Data input is one of the steps where IT fraud always is easy to happen, such as: to increase the number of deposit by inputting the artificial deposit bill; to make the artificial number of transaction by modifying the number of invoice in sale system.; to reflect the artificial number of stock by deleting the stock number in stock system; to make the artificial transaction record by connecting or interpreting the transmission system by hand.

To face the fraud during the data input, the internal control system must be set up, then the accuracy of the data resource can be assured by authorization and approve. In the program, the check module can be inserted to make sure the data is complete.

- **Data processing management.** Only after the data is preceded, the resource data can be used for the business system. During this step, data processing procedure and rules should be set up in the internal information system to prevent the fraud happen.

In IT environment, data processing procedures are usually done automatically in computers under the control of manpower. During this step, the control measures are mainly in the way of programs, such as: the business order controls. They will assure the order of the business under the confine of environment; the effective controls for the data file. It will check the validation of data, the length of the field and the record, the boundary of the value and whether virus affects the data; modification controls. In IT system, there must be the audit function of tracing the modification. In China, this function is weakened, thus it brings risk to auditors; confidentiality controls. In any case, the data should not be lost, destroyed, disclosed. It is the target of the data confidentiality. The measures include the ID check, the log keeping, data backup, read-only for the important data file, random key or encryption by hardware, etc.

- **Data output management.** If the data input and procession are well controlled, the data output management for the receiver aims to get the data timely and totally, while other people have no chance to access the data. The measures include: the authorization to transmit, print, and distribute the data; record the output and trace to check; the material keep of the data, such as electronic material or paper.

3. Software and communication controls.

IT fraud is a secret activity with IT; the fraud-maker can do it in the software and during the communication because they know more about IT than auditors.

- **Software management.** Such as: fraud is done by the external personnel. For instance, the developer installed the program of logic bomb in order to blackmail the customer. Some auditees installed the special program in order to grab the

privacy of the customers during the normal transactions; based on the customer's requirement, the software company leaves the backdoor for the customer to modify the data. There are leaks in the program that could not satisfy the control requirements. It is a challenge for not only the auditor but also the auditee to make the software management and controls. The IT specialists are needed during the check of the software functions.

- **Communication management.** At this step, the risks are:

Wiretapping. It is the description about the data security during the communication. In the end, the unauthorized personnel get the data.

Data integrity cannot be assured. The data is modified, disguised or destroyed through the weakness of the system or equipment.

There are some matured technologies in communication such as ID authentication (password/CA), encryption, VPN, etc. The controls should be put in two areas, one is to make suitable investment for equipment based on the importance of the business, thus the strong communication security is assured. The other is to set up strict management system and carry it out carefully. The statistics show that the weak password is the main reason for the credit card to be embezzled instead of cracking.

4. Hardware and environment management

In China, there is special organization that is responsible for checking the hardware, while the public security is responsible for the fireproofing and lighting proofing in computer room.

- **Hardware management.** The risks for hardware include the bad performance, the illegal program installed in hardware, poor redundancy and so on.

The suppliers with good honor should be selected in the purchasing step. The maintenance for the key hardware should not be out of the eyesight of the customers. There should be the approving and registration system for hardware.

- **Environment management.** The environment is the place where computers and its system are running. There are two points that should be paid attention to, one is access control to prevent the modification and destroy of data. The other is the disaster risk such as fire, flood and collapse.

The key of the environment management is to set and safeguard the security area to prevent the unauthorized access. It is important to have the entrance guard system which only permit the authorized personnel come in. it is necessary to install the alert the smoke, infrared warning, water and humid detector to assure the physical safety.

- **Equipment value management. The price of hardware is different. The main**

forms are:

- Price. Suppliers does not provide the hardware with good quality according to list when purchasing, the value of hardware is over evaluated and so on.
- Quantity. There is error in the number of hardware that will affect the whole value of equipment.
- Type. The error of the type will affect the accounting of the price.

It is almost same for the value management between IT and traditional environment. The difference is the management is more scattered.

5. Internet access management.

We must pay more attention to the internet access management while preventing and controlling IT fraud. Because of the Internet, the number of IT frauders increase, and the scope is enlarged. Some auditees even became an innocent organization who is imposed.

- **Access control.** It is necessary to have the effective access controls such as VPN, firewall and ID authorization.
- **Preventing hostile program.** The most common hostile program is virus, spy software and Trojan. The easy way to prevent the hostile program is to install the antivirus software and upgrade on time. For the unsure file, just delete it. It is also important not to log on the bad websites.
- **Preventing data disclosure.** In Internet, any data can be disclosed quickly. Besides access controls, killing the hostile program, enforcing management, water wall is another new technology that costs less with good result.

IT in China is only at the starting point, IT fraud- just likes the shadow- would be in the whole application. There are some new contents in finding the errors and checking the mistakes by using IT. The fighting between auditors and IT frauders would not stop. We are looking forward to more communication with other SAIs.