

IT Governance in China and CNAO'S FOCUS

CNAO (China National Audit Office)

CNAO prepares this country paper to the 5th Performance Audit Seminar. In this paper, we introduce the IT Governance in China. Based on the IT construction and the practice by CNAO, we also generalize the application of IT Governance Standards.

1. IT Governance is introduced, spread and applied in China.

There are two reasons for IT Governance to be introduced into China, one is the external reason, because the IT Governance Standards are matured; the other is the internal reason, the rapid development of IT Construction in China needs some standards.

CNAO believes that we can understand the concept of IT Governance from the following aspects:

- System target. The target of the IT project should be same as the businesses. IT should serve and drive the business.
- Economy. IT cost should be controlled to maximum the production capability; the investment should be helpful for the benefit.
- Change rapidly according to the requirements. IT section should follow the technology trend, but IT should not be the obstacle of the expending of the business.
- Continue the operation. Now IT has been the internal part of the business, so there must be some necessary measures to make sure the business could maintain in any case.
- Risk controls. Risk should be controlled during the whole processing, from the planning, implement, event management to the running, upgrade and so on.

Since 2000, IT Governance Standards are widely circulated and translated by the specialists, such as ITIL, COBIT, BS 7799, ISO/IEC17799 even ISO27001: 2005. These standards are having more and more impact.

1) ITIL.

ITIL is more preferred by the special IT companies who do the integration of the IT projects, because they find the projects couldn't play the function they should have if they just pass the projects to the customers. The disorder conditions in IT Section lead

to the failure. So IT companies try to persuade CEO and CIO to save the inefficient IT project by promising to improve the IT service management by using the best practice standards.

Some industries, such as the big-scale enterprises and government, which depend more on IT also pay more attention to ITIL. The famous IT Governance consulting provider-- CCID--gives more than 100 training classes for the Government, banks and Telecom company.

2) COBIT (Control Objectives for Information and related Technology)

Besides the same reason as ITIL in China, the concept of COBIT comes more from CISA (Certified Information System Auditor). ISACA began to go into China mainland since this century; as a result, COBIT comes into the eyesight of IT industry.

COBIT includes 4 domains, 34 process controls. It plays as both the ideal case for the implementation of IT projects, the standards to check whether the project is successful, and the reference to diagnose the faultiness of the project.

Although COBIT in china is only used in some industries, it still helps to improve the value of the IT project. In 2005, AIR CHINA applied the concept of IT Governance, integrated the internal IT resources, make the IT budget as a whole, share the information better and improve the business capability from IT.

3) ISO/IEC17799 (BS 7799) .

In April 2000, the first BS7799 seminar about the information security management system was hold in Xiamen, China. During discussion, the Norwegian specialists gave a lecture about the system of BS7799 and its latest developments. Later BS7799, ISO 17799 and ISO 27001:2005 were spread in China. Some Chinese enterprises are trying to pass the certification. In the end of 2004, 11 enterprises, including Huawei Technologies CO Ltd, Beijing Mobile Communication Co Ltd Mobile Date Center and etc, got the certification issued by BSI. In April 2006, Sino COM Software Group Limited got the first ISO 27001:2005 certification.

Based on the conditions in China, in the beginning of 2006, GB/T 20274.1-2006 Information Security Technology -Evaluation Framework for Information Systems Security Assurance, which is the information security management standard for chinese—was published.

2. The IT development needs the guide from IT Governance

If we use IT Governance as the criteria, there are still obvious gap in IT projects construction and operating management. We can explain as follows:

First, sometimes we didn't put the business requirements in the leading position.

IT was not the internal part of the strategy planning of the organization, the requirements were not very clear, the over attention of the IT driving made the business requirements put in the secondary position, the investment could not be changed into the production.

Secondly, CIO takes the place of CEO.

In China, IT project would fail if it could not get the support of the management. In contrast, some times CEO gives the whole project to CIO. But CIO pays more attention to the new technology and advanced equipments instead of the core competition. Furthermore, when the project involved the change of the management model, CIO would be helpless.

Thirdly, lack of overall planning.

China is a big country, so it is very difficult to make the overall planning. For instance, some CA were set up in China, but the certifications issued by different CA are not compatible each other. Another case: according to the audit survey, the state security system was separately managed by 400 cities; the data can not be exchanged fluently. This condition will lead to the integration difficulty in the future.

Fourthly, information is not sufficient shared.

In some organizations, the relationship between data capacity and the processing capacity of the equipments is not reasonable. Although they have advanced computer equipments, the database management is poor. All these made the share of information very difficult.

Fifthly, the output is not corresponded to the investment.

Compared with the huge investment, the output of IT project is hard to calculate. Actually we could not tell which comes uniquely from IT during the \$100 income. In fact, lots of IT projects especially the E-governance projects could not balance its investment and production.

Sixthly, the impact from IT was not estimated sufficiently.

Mr. LI Jinhua, the Auditor General of CNAO, once said that IT Audit is a kind of revolution. It means although auditors are skilled in the traditional audit environment, they will lose the certification if they could not master IT. It is same in other industries. IT will bring a lot of change in daily work. When an IT project comes, it is not enough only with IT engineers' passion, we need more involvement of the business departments and management.

Seventhly, the policy did not answer up according to the management control change

The improving efficiency comes from two reasons, one is the IT itself, another is the change of management. Once the change of the management control and adjust to the business flow are not considered carefully, there must be the conflict between the new project and the old ones. It usually leads to the failure of the project, furthermore, it would affect the development and survival of the organization.

Eighthly, the choice between the new technology and the matured one is not accurate

There are usually two mistakes during the choice between the new technology and the matured one. One is only pursuing the new technology, the other is the used technology does not matter with improving business capability. Some CIOs always could not help in purchasing the expensive advanced equipments without thinking about the rewards.

Ninthly, more hardware while less software, more construction while less maintenance, more technology while less management

According to the statistics in China, the ratio between the investment of software and hardware in China is 2:8. Among the investment, 80% for hardware, 8-10% for integration, 10-12% for software development. The operation and maintenance are not thought much. While the statistics made by World Bank shows that the ratio between the investment of software and hardware in developed cities is 7:3, namely 70% for software and service, 30% for hardware.

Tenthly, the emergency mechanism is needed. There are two reasons for the shortage of the measures; one is the shortage of fund. For instance, during the first term of the Golden Auditing Project of CNAO, the backup and disaster recovery was not included, we hope it can be resolved during the coming second term. In China, lots of organizations use this kind of way to solve the problem. The other is the lack of management routine for emergency, so the business could not continue successfully.

Last, the measures to avoid the failure are not effective.

Because of the high investment and risk, IT project is prone to fail if the measures to avoid the risk are not well considered. About 2/3 projects failed at last.

All above analysis come from three reasons, the first is CNAO's audit finding about the E-governance and IT project cause lots of attention, the second is we have got the valuable experiences through the work of Golden Auditing Project during last 5 years, the third is the self-reflection and the expectation.

We believe today's China is one part of the world; the reality in China must be the miniature of the world. The problems we just said are common, that is why CNAO decides to take part in the seminar.

3. CNAO's focus on IT Governance

Although we could not find a case that was totally designed according to the standards of ITIL or COBIT, we did not lose the confidence for IT Governance. We can borrow the experience to do our work. In China, IT Governance is regarded as not only the perfect requirement that should be followed as much as possible, but also the check reference we can use to make the recommendations for auditees.

CNAO's focus covers next three parts:

First, the supervision and check for the state e-governance projects.

In China, the feasibility report is necessary during the imitation of the e-governance project. In this report, besides the target, the investment, the function of the project, the economic benefit and the social benefit should also be explained. This report is also one of the important basis on which CNAO began its work. Now CNAO pays more attention to the supervision and check after the project is finished. It will check:

- Whether the target of e-governance is consistent with the business target.
- Whether the fund for the project is used rightly.
- Whether the project can get benefit from the investment.
- Whether it is easy to use after the finish of the project.

In 2006, CNAO disclosed the audit finding which are about the central e-government project. For instance, the value of \$9.6 million was not used from the beginning of the project in Finance Ministry, the Ministry of Land and Resource reapplied \$11.43 million, which had been included in the project, etc.

Secondly, the check and assessment of the reliability of the project.

Since the reform policy, to adapt to the production and competition environment, lots of state enterprises invested much on IT projects. The audit for the IT construction were also included, such as:

- Check whether the target of the IT project is consistent with the business target of the enterprise.

- Assess whether the system could support the business operation efficiently and continually.
- Analyze the cost and the benefit of the project.
- Check whether the fund resource is right and it is used legally.
- Whether the data provided from the information system is true.

In 2005, during CNAO's audit for an enterprise, we checked its financial management system. Through validating the safety and the confidentiality of the system, we found the version of the financial software used in the dispatched organization disagreed with each other, it led to the difficulty of sharing the data.

Thirdly, CNAO pays attention to the internal controls of auditees.

While using IT, organizations should also change its mechanism and measures to do its internal controls. Since the standards of IT Governance are the best practices requiring what to do and how to do, they can also play as the criteria for auditors to check the internal controls.

- To check whether the auditee has set up the effective internal controls through IT Governance.
- To check whether the internal controls could decrease the risk of big mistakes effectively.
- To summarize the new development and change of the risk-based audit in IT environment.

China is a developing country, where any theory that could help the economy develop healthily would be welcomed. This seminar can help auditors in CNAO understand IT Governance better and put the theory into their daily work.