IT Governance in China and the Chinese National Audit Office

This paper introduces IT Governance in China. Based on the IT construction and the practice by CNAO, we also generalize the application of IT Governance Standards.

IT Governance is introduced, spread and applied in China

There are two reasons for IT Governance to be introduced into China now, one is an external reason, because IT Governance Standards are mature; the other is an internal reason, the rapid development of IT systems in China need some standards. CNAO views IT Governance from the following angles:

System Objectives. The target of the IT project should be same as that of the business. IT should serve and drive the business.

Economy. The cost of IT should be controlled to maximise the production capability; the investment should be productive.

System Change. The IT section should follow technology trends, but IT should not be an obstacle to the expansion of the business.

Continuity. Once IT becomes an integral part of the business, there must be some necessary measures to make sure the business can continue in any case.

Risk controls. Risk should be controlled during the whole process, from the planning, implementation, event management to the live running and upgrade.

Since 2000, specialists have widely translated and circulated IT Governance Standards, such as ITIL, COBIT, BS 7799, ISO/IEC17799 and even ISO27001: 2005. These standards are having more and more impact.
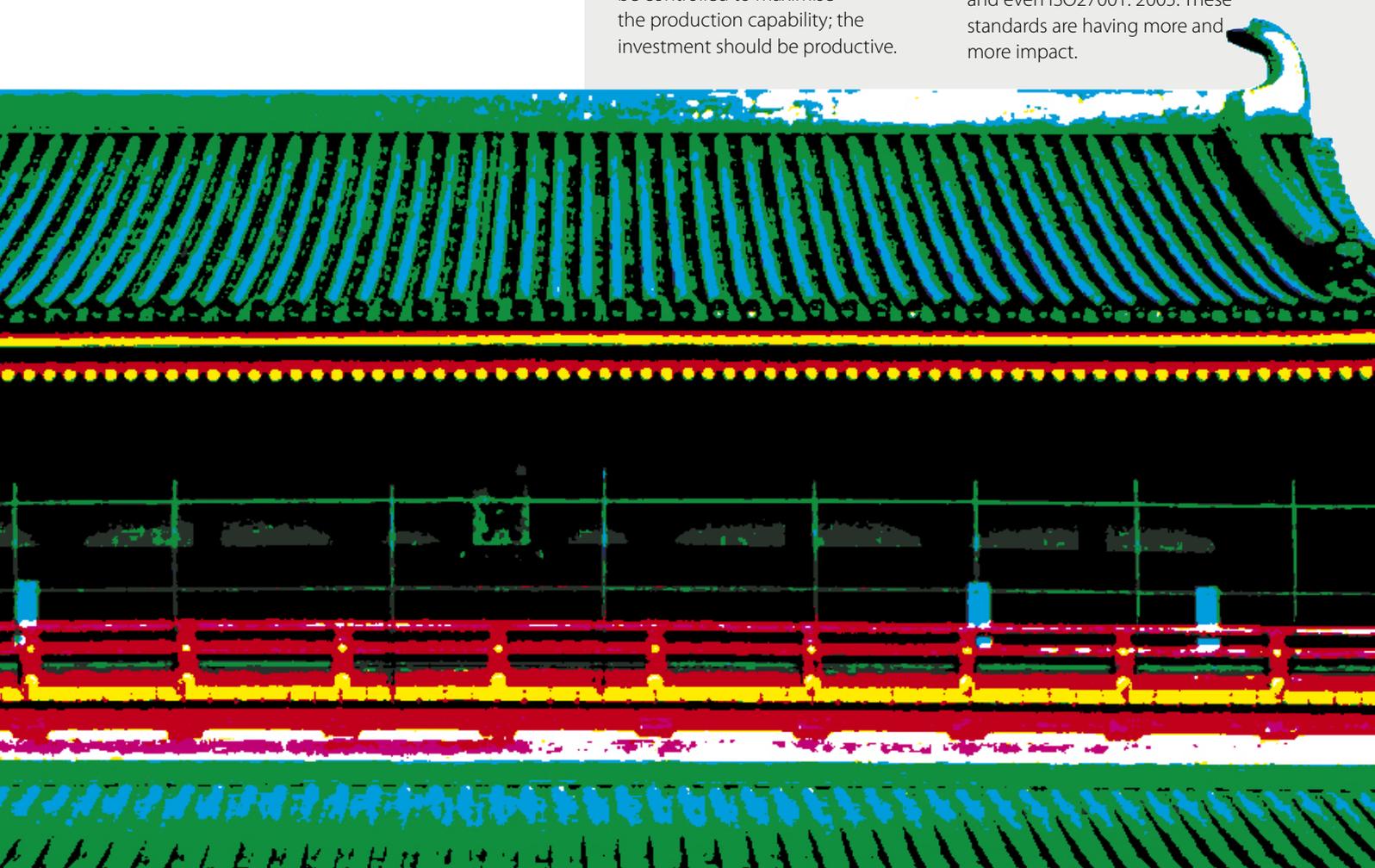
BY **MR. WANG ZHIYU**, DIRECTOR GENERAL, IT CENTRE, CHINA
NATIONAL AUDIT OFFICE AND TRANSLATED BY MS. YANG LI

ITIL

ITIL is preferred by the special IT companies who carry out the integration of IT projects. They find the projects could not perform the function they should have if they just pass the projects to the customers. The disorganised conditions in the IT Section lead to failure. So IT companies try to persuade senior management to save the inefficient IT project by promising to improve the IT service management by using the best practice standards.

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

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

ISACA became active in China at the turn of this century, and with it COBIT became visible to the IT industry.

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 concepts of IT Governance, and used COBIT to improve its business capability with IT, integrating its internal IT budget and other resources and sharing its information better.

ISO/IEC17799 (BS 7799)

In April 2000, the first BS7799 seminar about this information security management system was held in Xiamen, China. During this seminar Norwegian specialists gave a lecture about BS7799 and its most recent developments. Later BS7799, ISO 17799 and ISO 27001:2005 were spread in China. Some Chinese enterprises are trying to gain certification, at the end of 2004, 11 enterprises, including Huawei Technologies Co. Ltd, Beijing Mobile Communication Co Ltd, Mobile Date Center and others, won the certification issued by BSI. In April 2006, Sino COM Software Group Limited won 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.
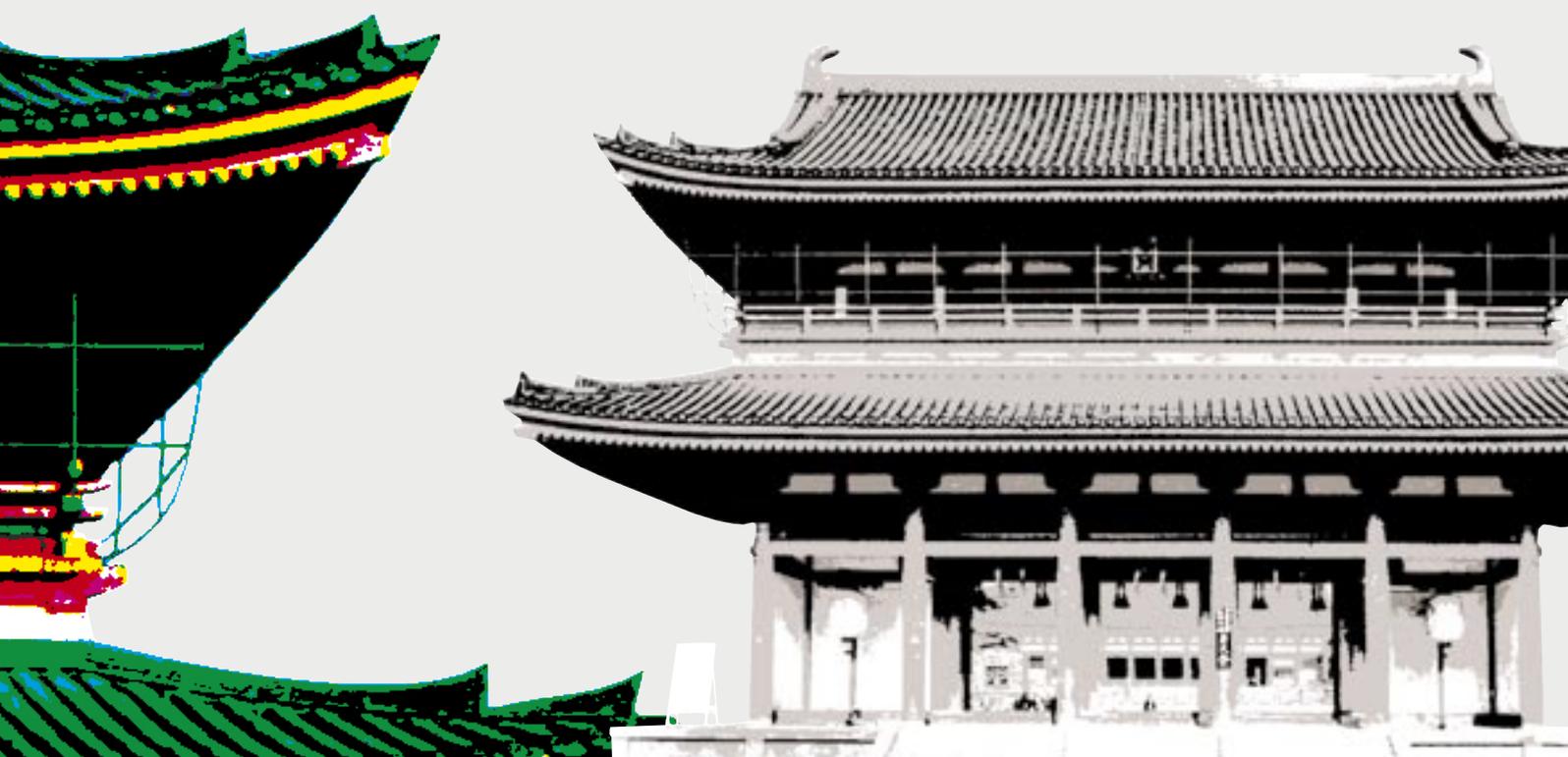
The IT development needs the guide from IT Governance

Using IT Governance as the criteria, there are still obvious gaps in IT project construction and operating management. We can explain as follows:

1 Sometimes we did not give enough priority to business requirements. IT was not part of the organisation's strategic plan, the requirements were not very clear, an over-attention to the technical aspects of IT put business requirements into a secondary position.

2 The CIO leads the project rather than the CEO. In China, an IT project would fail if it could not get the support of the management. In contrast, the CEO might give the whole project to the CIO. But typically, the CIO pays more attention to the new technology and advanced equipment rather than the core components. Furthermore, if the project involved a change in the management model, the CIO would be helpless.

3 A lack of overall planning. China is a big country, so it is very difficult to make the overall planning. For instance, some Certification Authorities (CA) were set up in China, but the certifications issued by different CAs are not compatible each other. In another case, according to the audit survey, the state security system was separately managed by 400 cities and the data can not be exchanged easily. This condition will lead to integration difficulties in the future.

4 Information is not adequately shared. In some organizations, the relationship between data capacity and the processing capacity of the equipment is not reasonable. Although they have advanced computer equipment, the database management is poor. All these made the sharing information very difficult.

5 The output does not correspond to the investment. Despite a huge investment in IT, the output of the project is hard to calculate. Actually we could not tell what part of the output comes uniquely from IT. In fact, lots of IT projects especially the E-governance projects could not balance their investment and production.

6 The impact from IT was not estimated sufficiently. Mr. LI Jinhua, the Auditor General of CNAO, has 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 cannot master IT. As in other industries IT will bring a lot of changes to the daily work. When an IT project comes, it is not enough to rely simply on the passion of IT engineers, we need more involvement from the business departments and management.

7 The strategy did not identify necessary changes to management controls. Improvements in efficiency come from two sources, one is the IT itself, another is the change of management. If the change to management and adjustments to business flows are not considered carefully, there will be conflict between the new project and the old ways. This usually leads to the failure of the project, and furthermore, can affect the development and survival of the organization.

8 The choice between the new and mature technologies is not considered properly. There are usually two mistakes made when choosing between new and mature technologies. One is only pursing the new technology, the other is using technology that does not help to improve business capability. Some CIOs purchase expensive advanced equipment without considering the rewards.

9 More hardware but less software, more construction with less maintenance, more technology with less management. According to statistics in China, the ratio between the investment of software and hardware is 2:8. That is, 80% for hardware, 8-10% for integration and 10-12% for software development. Operational and maintenance costs are not given sufficient weight. While the statistics from the World Bank show that the ratio between the investment of software and hardware in developed cities is 7:3, i.e. 70% for software and services, 30% for hardware.

10 An emergency recovery mechanism is needed. There are two reasons for a lack of such mechanisms. One is a shortage of funds. For example, during the first term of the CNAO's Golden Auditing Project, backup and disaster recovery were not included, although we hope it can be resolved during the coming second phase. In China, lots of organizations follow this pattern. The other reason is a lack of management routines for disaster recovery, so the business cannot continue successfully.

Finally The measures to avoid failure are not effective. Because of the large investment and high risk, IT projects are prone to fail if the risk management is not well considered. About two thirds of projects failed in the end.

All the points above come from three sources. The first is CNAO's audit findings about E-governance and IT projects which generates a lot of attention. The second is the valuable experience we have gained from the work of Golden Auditing Project during last 5 years. The third is self-reflection and expectations.

We believe today's China is part of one world; the reality in China must be the miniature of the world. The problems are common.

CNAO's focus on IT Governance

Although we could not find a example project that was totally designed according to the standards of ITIL or COBIT, we did not lose confidence in 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 recommendations to auditees.

CNAO's focus covers three parts:

1   **The supervision and check of public sector e-governance projects**. In China, a feasibility study must be made during the initiation phase of an e-governance project. In this, the economic and social benefit should be explained as well as the target, investment and function of the project. This is also one of the important fundamentals from which the CNAO begins 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 funds for the project are applied correctly.

- Whether the project deliver benefits from the investment.

- Whether the delivered systems are easy to use.

In 2006, CNAO published its audit findings about the central e-government project. For example, $9.6 million was not used from the beginning of the project in the Finance Ministry, the Ministry of Land and Resource reapplied $11.43 million, which had been included in the project, etc.

2   **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 have invested much on IT projects. The audit for the IT construction were also included, such as:

- Check whether the objectives of the IT project are consistent with the business objectives of the enterprise.

- Assess whether the system can support the business operation efficiently and continually.

- Analyze the cost and the benefits of the project.

- Check whether the funding is correct and used legally.

- Check whether the data provided from the information system is accurate.

In 2005, during CNAO's audit of an enterprise, we checked its financial management system. Through validating the security and confidentiality of the system, we found that versions of the financial software used in the dispatched organization were incompatible, and this led to difficulties in sharing data.

3   **CNAO pays attention to the internal controls of auditees**. While using IT, organisations should also change their mechanisms and methods to maintain their internal controls. Standards of IT Governance are best practice setting out what and how to do, so auditors can use the as the criteria when checking internal controls.

- To check whether the auditee has set up effective internal controls through IT Governance.

- To check whether 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. These can help CNAO auditors to understand IT Governance better and put the theory into their daily work.

Biographical notes

Mr. WANG Zhiyu was born in 1953. He graduated from ZHENG ZHOU University and got the Bachelor of Economy Science in 1981.

He was the member of the Preparing Team of China National Audit Office in 1983. And then he worked as the secretary of Auditor General, Deputy Director of Laws Department, Deputy Director General of Audit Administration Department, Deputy Director General of Agriculture and Resource Protection Audit Department.

Since 1999, He became the Director General of IT Center. As CIO, now he is responsible for the Golden Auditing Project. Because of his excellent work, he was awarded Outstanding Contribution for Pushing the Application of IT in China in 2004.