

ICS 03.060
CCS A 11

JR

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

JR/T 0073-2012

**Testing and evaluation service security guide for classified
protection of information security of financial industry
(English Translation)**

Issued on: July 6, 2012

Implemented on: July 6, 2012

**Issued by: People's Bank of China 3. No action is required - Full-copy of
this standard will be automatically & immediate**

Table of Contents

Preface...	3
Foreword...	4
1 Scope...	5
2 Normative references...	5
3 Qualification requirements...	5
4 Assessment process requirements...	8

Foreword

The important information system in financial industry is related to national economy and the people's livelihood, and is the key target of national information security protection. Therefore, financial industry is one of the key industries for implementing information security classified protection. Due to the fact that most of the information systems in financial industry are technology-intensive, capital-intensive, complex and networked man-machine systems, carrying out testing and evaluation for classified protection of information security of information systems in financial industry requires a batch of assessment organizations who can understand business systems in financial industry and have a strong technical ability to carry out evaluation. In financial industry the information system, classified as three or four level, is related to the important system of national economy and people's livelihood. It is of great significance for ensuring the safe and stable operation of important information system and stabilization of national economy and the people's livelihood to effectively avoid the existing risk of classified protection evaluation. Therefore, the restraint and standardization for assessment organizations are important parts of implementing classified protection in financial industry.

To this end, People's Bank of China has formulated "Testing and evaluation service security guide for classified protection of information security of financial

industry" (hereinafter referred to as "Security Guide") to clarify the basic requirements of agency safety, personnel safety, process safety, testing objects safety, and tool safety; and to guide assessment organizations of classified protection to carry out testing and evaluation of information system security classified protection in financial institutions.

Testing and evaluation service security guide for classified
protection of information security of financial industry

1 Scope

This standard summarizes the security needs and the business characteristics of financial industry application system of many years, clarifies the basic requirements of agency safety, personnel safety, process safety, testing objects safety, and tool safety with reference to international-domestic related information security standards and industry standards.

This standard applies to the third party (hereinafter referred to as assessment organization) of which the information security departments engaging in the information systems of financial industry carry out information security classified protection evaluation, and the supervision-management of personnel and evaluation activities.

2 Normative references

The following documents are essential for the application of this document. For dated references, only those dated references apply to this document. For undated references, the latest edition (including all amendments) applies to this document.

Public-Communication-Letter [2007] No.43 Management Measures of
Information Security Classified Protection

3.1 Qualification requirements of assessment organizations

The third-party agency engaging in the testing and evaluation of information security classified protection of financial industry information system shall have and comply with the following qualification requirements.

- a) Have the qualification of the testing and evaluation of information security classified protection approved by Ministry of Public Security, and is recommended by Ministry of Public Security for being the assessment organization of classified protection;
- b) The relationship of property rights is clear, and registered capital is no less than 5 million yuan;
- c) Have the certificate of accreditation from China National Accreditation Service for Conformity Assessment (CNAS) laboratories or inspection agencies;
- d) Have more than 2 years working experience in information system security evaluation and have conducted information system security evaluation of financial institutions at least once within the recent one year;
- e) There are no bad records in legal dispute, rules-violation records, major information security breaches or other major security incidents during the evaluation work of the recent 5 years;
- f) The proportion of academic qualifications in evaluation institutions shall be no less than 60% of undergraduate degree or above;
- g) The staffs of evaluation institutions shall be no less than 30 in number; the professional and technical personnel and management personnel shall be no less than 20, who meet the needs of classified evaluation work; technical appraisers shall be no less than 15.

3.2 Management requirements of assessment organizations

The third-party agency engaging in the testing and evaluation of information security classified protection of financial industry information system shall have and comply with the following management requirements.

- a) Assessment organizations and its assessors shall strictly implement the relevant standards on classified protection of national information security and the relevant provisions in financial industry; provide objective, fair, just and effective classified protection evaluation service and bear the corresponding legal responsibilities;
- b) There should be a quality system that ensures its impartiality and independence, and ensure that the evaluation activities are free from any commercial or financial pressure that may affect the outcome of the evaluation.
- c) The job configuration of assessment organizations shall be equipped with at least evaluation technician, project manager, technical supervisor, quality supervisor, confidential security officer and archivist. Among them, project managers, technical supervisors, quality supervisors, confidential
 - a) The assessment tools used must be authorized edition within the validity period; pirated software can not be used.
 - b) The assessment tools used shall give priority to the use of similar products with independent intellectual property rights in China, on the premise of meeting the requirements in function and performance.
 - c) The manufacturer of the assessment tools used shall be a regular manufacturer, have certain capabilities of R&D and service, be able to continuously update the products and provide quality and safety assurance;
 - d) The assessment tools used by assessment organizations will not have any destruction or negative impact on the system.