

ICS 03.060
CCS A 11

JR

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

JR/T 0071-2012

**Implementation guide for classified protection of information
system of financial industry**

金融行业信息系统信息安全等级保护实施指引

(English Translation)

Issued on: July 6, 2012

Implemented on: July 6, 2012

Issued by: The People's Bank of China Foreword

.....

Table of Contents

Foreword	4
Introduction	5
1 Scope	6
2 Normative references	6
3 Terms and definitions	8
3.1 Sensitive data	8
3.2 Risk	8
3.3 Security policy	8
3.4 Security requirement	9
3.5 Integrity	9
3.6 Availability	9
3.7 Weak password	9
4 Guide Preparation Policy	9
4.1 National requirements of classified protection	9
4.1.1 Basic requirements	10
4.1.2 Design requirements	12
4.2 Guidelines	13
4.2.1 Necessity of defense-in-depth design defense-in-depth design	15
5 Information Security Assurance Framework	16
5.1 General	16
5.2 Technical system	18
5.2.1 Computing environment	19
5.2.2 Zone boundary	21
5.2.3 Communication network	22
5.2.4 Supporting facilities	22
5.3 Management system	22
6 Protection Requirements	24
6.1 Level II requirements	24
6.1.1 Technical requirements	24
6.1.2 Management requirements	32
6.2 Level III requirements	48
6.2.1 Technical requirements	48

6.2.2 Management Requirements	65
6.3 Level IV requirements	90
6.3.1 Technical requirements	90
6.3.2 Management requirements	109
A.1 Network security	137
A.1.1 Level II requirements and measures	137
A.1.2 Level III requirements and measures	145
A.1.3 Level IV requirements and measures	158
A.2 Host security	171
A.2.1 Level II requirements and measures	171
A.2.2 Level III requirements and measures	177
A.2.3 Level IV requirements and measures	186
A.3 Application security	196
A.3.1 Level II requirements and measures	196
A.3.2 Level III requirements and measures	201
A.3.3 Level IV requirements and measures	209
A.4 Data security	219
A.4.1 Level II requirements and measures	219
A.4.2 Level III requirements and measures	220
A.4.3 Level IV requirements and measures	222
Industry and the Use Instructions	225
Bibliography	229

1 Scope

According to the national standards "Baseline for Classified Protection of Information System Security ", "Technical Requirements of Security Design for Information System Classified Protection", and the characteristics of financial industry and requirements for information systems security development, this

Standard has designed the information security system structure in divisions and has specified the application systems depending on the system level, so as to guarantee industrialized and concretized national requirements for classified protection, and to improve the protection level of information security for the important networks and information systems of our bank.

This Standard is applicable to the use by the departments of financial institution (including

its affiliates), e.g. system planning and development (service and technology), application development, system operation, security management, system use, internal supervision and audit. It may be served as the basis for the supervision, inspection and guidance for information security functions.

With the supplementing and enrichment of the contents, this Standard provides guidance for the practice of classified protection.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB/T 22239-2008 Baseline for Classified Protection of Information System
Security

GB/T 25069 Information Security Technology - Glossary

JR/T 0003-2001 Security Specification for the Interoperable Services of
Bank Card

JR/T 0013-2004 Specification on the Interconnection Security between
Star Networks of Financial Industry

JR/T 0011-2004 Systematic Specification of Centralized Bank Data Center

JR/T 0023-2004 Specification on Information Technology Management of
Securities Company

JR/T 0026-2006 Specification for Protection against Lightning of Banking
Computer Information System

JR/T 0044-2008 Management Specification of Information System
Disaster Recovery for Banks

JR/T 0055.4-2009 Technical Specifications on Bankcard Interoperability -
Part 4: Data Secure Transmission Control

PBC Doc. [2002] No. 260 Guidance of the People's Bank of China on
Reinforcing Bank Data Concentration Security

YIN KE JI [2006] No. 73 Guidance of the People's Bank of China on the
Secure Configuration of Information System

YIN BAN Doc. [2006] No. 154 Guidance of the People's Bank of China on IT Emergency Plan

YIN BAN Doc. [2006] No. 9 Guidance of the People's Bank of China on the Normalization of Computer Room

PBC Doc. [2010] No. 276 Administrative Rules of the People's Bank of China on Computer System Information Security

PBC Doc. [2010] No. 276 Administrative Rules of the People's Bank of China on Computer System Information Security

CBRC Doc. [2008] No. 50 Administrative Regulations on the Commissioning and Modification of Important Information Systems of Banking Financial Institutions

CBRC [2009] No. 19 Guidance on the Information Technology Risk Management for Commercial Banks

YIN JIAN BAN Doc. [2009] No. 437 Guidance on Emergency Handling for Cross-industry Information System of Banking and Securities

YIN JIAN BAN Doc. [2010] No. 112 Guidance on the Supervision of Commercial Bank Data Center

SAC Doc. [2006] Guidance on the Security Management Technology of Centralized Transaction for Securities Companies

3.4 Security requirement

The protection class and protection level required in order to meet the security policy requirements for equipment, information, application and installation.

3.5 Integrity

It covers data integrity and system integrity. The data integrity characterizes data, i.e. the degree that the accuracy and consistency of data keep unchanged no matter how its form changes; the system integrity characterize the performance of system in fulfilling operation intention when preventing unauthorized user from modification or use of resource and preventing authorized user from improper modification or use of resource.