

ICS 03.060
CCS A 11

JR

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

JR/T 0072-2012

**Testing and evaluation 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测评指南

(English Translation)

Issued on: July 6, 2012

Implemented on: July 6, 2012

Issued by: THE PEOPLE'S BANK OF CHINA

Table of Contents

Foreword	6
Introduction	7
1 Scope	8
2 Normative references	8
3 Overview	9
3.1 Evaluation contents	9
3.2 Evaluation object	10
3.3 Evaluation index	10
3.4 Evaluation method	10
3.4.1 Field evaluation method	11
3.4.2 Risk analysis method	11
3.5 Class-evaluation risk	12
3.5.1 Verification evaluation that impacts normal operation of system	12
3.5.2 Tool evaluation that impacts normal operation of system	12
3.5.3 Sensitive information leakage	12
4 Class-evaluation process	12
4.1 Evaluation preparation	12
4.2 Program preparation	13
4.3 Field evaluation activity	13
4.4 Analysis and report preparation activity	13
5 Evaluation preparation	13
5.1 Project initiation	13
5.2 Information collection and analysis	14
5.3 Tools and forms preparation	14
6 Evaluation program	14
6.1 Determination of evaluation object	14
6.2 Determination of evaluation indexes system: system:	17
6.3 Determination of evaluation tool's access-point	17
6.4 Determination of unit-evaluation content	18
6.5 Evaluation program preparation	18
7 Field evaluation	19
7.1 Unit-evaluation	19

7.1.1 Unit-evaluation for second-level information system	19
7.1.1.1 Security technology evaluation	19
7.1.1.1.1 Physical security	19
7.1.1.1.2 Network security	30
7.1.1.1.3 Host security	37
7.1.1.1.4 Application security	45
7.1.1.1.5 Data security and backup recovery	53
7.1.1.2 Security management evaluation	57
7.1.1.2.1 Security management system	57
7.1.1.2.2 Security management institution	60
7.1.1.2.3 Personnel security management	65
7.1.1.2.4 System construction management	70
7.1.1.2.5 System operation-maintenance management	80
7.1.2 Unit-evaluation for third-level information system	97
7.1.2.1 Security technology evaluation	97
7.1.2.1.1 Physical security	97
7.1.2.1.2 Network security	113
7.1.2.1.3 Host security	123
7.1.2.1.4 Application security	136
7.1.2.1.5 Data security and backup recovery	148
7.1.2.2 Security management evaluation	153
7.1.2.2.1 Security management system	153
7.1.2.2.2 Security management mechanism	156
7.1.2.2.3 Personnel security management	165
7.1.2.2.4 System construction management	171
7.1.2.2.5 System operation management	186
7.1.3 Unit-evaluation for fourth-level information system	210
7.1.3.1 Security technology evaluation	210
7.1.3.1.1 Physical security	210
7.1.3.1.2 Network security	228
7.1.3.1.3 Host security	240
7.1.3.1.4 Application security	254
7.1.3.2 Security management evaluation	274
7.1.3.2.1 Security management system	274
7.1.3.2.2 Security management institution	278

7.1.3.2.3 Staff security management	287
7.1.3.2.4 System construction management	294
7.1.3.2.5 System operation and maintenance management	310
7.2 Overall evaluation	338
7.2.1 Evaluation among security control points	338
7.2.2 Inter-levels security evaluation	339
7.2.3 Inter-areas security evaluation	340
7.2.4 System structure security evaluation	341
8 Analysis and report preparation	342
8.1 Result judgment of unit-evaluation	342
8.2 Summary of unit-evaluation result	342
8.3 Summary of overall evaluation result	343
8.3.1 Inter-controls security evaluation	343
8.3.2 Inter-levels security evaluation	344
8.3.3 Inter-areas security evaluation	344
8.4 Risk analysis and assessment	345
8.5 Class-evaluation conclusion	345
8.6 Security construction and corrective action recommendations	346
Annex A (Informative annex) Field unit-evaluation checklist	347
A.1 Second-level information system checklist	347
A.1.1 Technical checklist	347
A.1.1.1 Physical security checklist	347
A.1.1.2 Network security checklist	352
A.1.1.3 Host security checklist	356
A.1.1.4 Application security checklist	362
A.1.1.5 Data security checklist	372
A.1.2 Management checklist	374
A.1.2.1 Security management system	374
A.1.2.2 Security management institution	376
A.1.2.3 Personnel security management	378
A.1.2.4 System construction management	381
A.1.2.5 System operation management	390
A.2 Third-level information system checklist	405
A.2.1 Technical checklist	405
A.2.1.1 Physical security checklist	405

A.2.1.2 Network security checklist	415
A.2.1.3 Host security checklist	421
A.2.1.4 Application security checklist	430
A.2.1.5 Data security checklist	441
A.2.2 Management checklist	443
A.2.2.1 Security management system	443
A.2.2.2 Security management institution	446
A.2.2.3 Personnel security management	452
A.2.2.4 System construction management	456
A.2.2.5 System operation and maintenance management	466
A.3 Fourth-level information system checklist	490
A.3.1 Technical checklist	490
A.3.1.1 Physical security checklist	490
A.3.1.2 Network security checklist	501
A.3.1.3 Host security checklist	508
A.3.1.4 Application security checklist	517
A.3.1.5 Data security checklist	529
A.3.2 Management checklist	532
A.3.2.1 Security management system	532
A.3.2.2 Security management institution	535
A.3.2.3 Personnel security management	543
A.3.2.4 System construction management	547
A.3.2.5 System operation management	559
Bibliography	590

1 Scope

This Standard specifies the requirements for classified protection of information system of financial industry, including unit-evaluation requirements for security evaluation of second-level information system, third-level information system and fourth-level information system and overall evaluation system of information system, etc. Based on the classification of information system of financial industry, fifth-level system does not exist, while first-level system is not required to file at public security agency, and it is not the key point of evaluation. This Standard omits specific content requirements for unit-evaluation of first-level information system and fifth-level information system.

This Standard applies to the industry to perform self-evaluation (e.g. second-level