

ICS 03.060
CCS A 11

JR

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

JR/T 0071.2-2020

**Implementation guidelines for classified protection of
cybersecurity of the financial industry - Part 2: Basic
Requirements
(English Translation)**

Issued on: January 1, 1970

Implemented on: November 11, 2020

Issued by: People's Bank of China

Table of Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

Foreword

JR/T 0071 "Guidelines for the Implementation of Cyber Security Graded Protection in the Financial Industry" is divided into six parts.

--Part 1: Basics and terminology;

--Part 2: Basic requirements;

--Part 3: Job ability requirements and evaluation guidelines;

--Part 4: Training Guidelines;

--Part 5: Audit requirements;

--Part 6: Audit Guidelines.

This part is part 2 of JR/T 0071.

This part was drafted in accordance with the rules given in GB/T 1.1-2009.

This part replaces JR/T 0071-2012 "Guidelines for the Implementation of Information Security Level Protection of Information Systems in the Financial Industry", and is in line with JR/T 0071-2012 in comparison, the main technical changes are as follows.

-Added "Overview of Network Security Level Protection" (see Chapter 5);

-Modified the "Network Security Assurance Framework" (see Chapter 6, Chapter 5 of the 2012 edition);

--Modified the "secure physical environment", "secure communication network", "security" in the "security general requirements" of the "second level security requirements" "Regional Boundary", "Secure Computing Environment", "Security Management Center", "Security Management System", "Security Management Organization", "Security Management Staff" "Safety construction management" and "safe operation and maintenance management" related requirements (see 7.1, 2012 version 6.1);

--Added "Cloud Computing Security Extension Requirements", "Mobile Internet Security Extension Requirements", and "Internet of Things Security Requirements" in the "Second Level Security Requirements".

Full extension requirements" (see Chapter 7);

--Modified the "safe physical environment", "safe communication network" and "safety" in the "safety general requirements" of the "third level safety requirements".

"Regional Boundary", "Secure Computing Environment", "Security Management Center", "Security Management System", "Security Management Organization", "Security Management Staff" "Safety construction management" and "safe operation and maintenance management" related requirements (see 8.1, 2012 edition 6.2);

--- Added "Cloud Computing Security Extension Requirements", "Mobile Internet Security Extension Requirements", and "Internet of Things Security Requirements" in the "Third Level Security Requirements".

Full extension requirements" (see Chapter 8);

--Modified the "safe physical environment", "safe communication network", "safety" in the "safety general requirements" of the "fourth level of safety requirements" "Regional Boundary", "Secure Computing Environment", "Security Management Center", "Security Management System", "Security Management Organization", "Security Management Staff" "Safety construction management" and "safe operation and maintenance management" related requirements (see 9.1, 2012 edition 6.3);

- Added "Cloud Computing Security Extension Requirements", "Mobile Internet Security Extension Requirements", and "Internet of Things Security Requirements" in "Level 4 Security Requirements".

Full extension requirements" (see Chapter 9);

-Deleted "Level Protection Implementation Measures" (2012 edition Appendix A);

-Revised the "Instructions for the Selection and Use of Security Requirements for the Financial Industry" (see Appendix A, Appendix B of the 2012 edition);

--- Added "Requirements on the overall security protection capabilities of hierarchical protected objects" (see Appendix B);

--- Added the "level protection security framework and key technology use requirements" (see Appendix C);

-Added "Cloud computing application scenario description, security management responsibility subject under different cloud service modes" (see Appendix D);

-Added "Mobile Internet Application Scenario Description" (see Appendix E);

- Added "Internet of Things Application Scenario Description" (see Appendix F);
- Added "Big Data Application Scenario Description" (see Appendix G);
- Added "sensitive data and personal financial information categories" (see Appendix H).

This part was proposed by the People's Bank of China.

This part is under the jurisdiction of the National Financial Standardization Technical Committee (SAC/TC 180).

Drafting organizations of this section. the Department of Science and Technology of the People's Bank of China, the Statistical Information and Risk Monitoring Department of China Banking and Insurance Regulatory Commission, China China Financial Electronics Corporation, Beijing Zhongjin Guosheng Certification Co., Ltd., Bank Card Testing Center, China Ping An Insurance (Group) Co., Ltd.

Division, Beijing Tianrongxin Network Security Technology Co., Ltd., Huawei Technologies Co., Ltd., Business Management Department of the People's Bank of China, People's Bank of China Guangzhou Branch, Digital Currency Research Institute of the People's Bank of China, Financial Information Center of the People's Bank of China, Guotai Junan Securities Co., Ltd., China Life Insurance Co., Ltd., People's Insurance Company of China, Industrial and Commercial Bank of China Co., Ltd., Agricultural Bank of China Co., Ltd., Bank of China Co., Ltd., China Construction Bank Co., Ltd., Bank of Communications Co., Ltd., Ant Branch Technology Group Co., Ltd., China Financial Certification Center, AsiaInfo Security Technology Co., Ltd.

Introduction

The level of cyber security protection is a basic system for the national cyber security assurance work. Important systems in the financial industry are related to the national economy and the people's livelihood.

It is the key protection object of national network security, so it needs a series of grade protection standard systems suitable for the financial industry as the support to standardize and Guide the implementation of hierarchical protection in the financial industry. With the widespread application of new technologies such as cloud computing, mobile internet, Internet of Things, and big data, the Golden Financial institutions are continuing to promote the transformation of IT architecture in accordance with their own development needs. In order to adapt to new technologies, new applications and new architectures the development of the industry's cyber security level protection work is now revising JR/T 0071. The revised JR/T 0071 is based on national cyber security Level protection related requirements, provide methodology, specific construction measures and technical guidance for the financial industry's network security construction, and improve the financial industry the industrial network security level protection system is better adapted to the application of

new technologies in the financial industry.

Guidelines for the Implementation of Levels of Cybersecurity Protection in the Financial Industry Part 2: Basic requirements

1 Scope

This part regulates the network security assurance framework of the financial industry and the security requirements corresponding to different security levels.

This part is applicable to guide financial institutions, evaluation institutions, and financial industry cybersecurity level protection authorities to implement cybersecurity levels Protection work.

2 Normative references

The following documents are indispensable for the application of this document. For dated reference documents, only the dated version applies to this document.

For undated reference documents, the latest version (including all amendments) is applicable to this document.

GB/T 22239-2019 Information Security Technology Network Security Level Protection Basic Requirements GB/T 22240-2020 Information Security Technology Network Security Level Protection Rating Guidelines GB/T 25070-2019 Information Security Technology, Cyber Security Level Protection Security Design Technical Requirements GB/T 31167-2014 Information Security Technology Cloud Computing Service Security Guidelines GB/T 31168-2014 Information Security Technology Cloud Computing Service Security Capability Requirements GB/T 32400-2015 Information Technology Cloud Computing Overview and Vocabulary GM/T 0054-2018 Information system password application basic requirements JR/T 0171-2020 Personal Financial Information Protection Technical Specification

3 Terms and definitions

The following terms and definitions apply to this document.

Cybersecurity

By taking necessary measures to prevent attacks, intrusions, interference, sabotage, illegal use, and accidents on the network, make the network in the state of stable and reliable operation, and the ability to ensure the integrity, confidentiality, and availability of network data.

[GB/T 22239-2019, definition 3.1] 3.2 Classified system A system that has determined the level of security protection.

Note 1: The grading system is divided into the first-level, second-level, third-level, fourth-level and