

ICS 03.060
CCS A 11

JR

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

JR/T 0071.4-2020

**Implementation guidelines for classified protection of
cybersecurity of the financial industry - Part 4: Guidelines for
training**

(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 Training objectives	
4 Training principles	
5 Training plan	
6 Trainees	
7 Training content requirements	
8 Training implementation	
9 Training and assessment	
9.1 Training and assessment basis and requirements	
9.2 Implementation of training and assessment	
9.3 Training assessment results	
9.4 Treatment of unqualified training assessment	
10 Training file management	

Foreword

JR/T 0071 "Implementation Guidelines for Cyber Security Graded Protection in the Financial Industry" consists of the following 6 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 4 of JR/T 0071.

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

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 Financial Electronics Corporation, Beijing Zhongjin Guosheng Certification 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 the new technology, new application and new structure, the financial bank for the development of industrial network security level protection, JR/T 0071 is now revised. The revised JR/T 0071 is based on the national cyber security level Protect relevant requirements, provide methodology, specific construction measures and technical guidance for the financial industry's network security construction, and improve the financial industry's network the 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 4: Training Guidelines

1 Scope

This part specifies the training objectives, training principles, training plans, training targets, training content requirements, and training practices for cybersecurity training.

Implementation, training assessment and training file management.

This part is applicable to financial institutions, evaluation institutions and financial industry cybersecurity level protection departments that implement cybersecurity level protection Gate.

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 20269 Information Security Technology Information System Security Management Requirements
GB/T 22239 Information Security Technology Network Security Level Protection Basic Requirements
GB/T 25058 Information Security Technology Network Security Level Protection Implementation Guide
GB/T 28448 Information Security Technology Network Security Level Protection Evaluation Requirements

3 Training objectives

In accordance with the requirements of GB/T 20269, GB/T 22239, GB/T 25058, GB/T 28448, financial institutions should carry out cyber security training jobs. Through the implementation of network security training in the financial industry, relevant personnel of financial institutions have basic knowledge of network security level protection and network security all basic knowledge and skills provide human resources guarantee for financial institutions to effectively implement the level of network security protection.

4 Training principles

Training should follow the following principles.

- a) Combination of personal skills training and corporate training.
- b) Short-term training is the main focus, and long-term training is the supplement.
- c) Carry out diversified training based on the needs of relevant positions for network security level protection.

5 Training plan

The training plan should include the following.

- a) Annual training plan. In order to implement the requirements of the cyber security level protection system, financial institutions should formulate an annual cyber security training plan.

Plan, focusing on the training of management personnel and new recruits related to network security level protection. Annual cyber security training should be accepted Enter the overall annual training plan of the institution.

b) Plan requirements. The training plan should specify training objectives, training content, training time, participants in training, methods, training Required resources, training budget and assessment requirements, etc.

6 Trainees

Based on the corresponding job requirements of the organization's cyber security level protection, the training objects mainly include management personnel and cyber security level protection Implementation personnel and other related personnel (or departments).

a) Institutional management. mainly includes members of the board of directors, chief executive officer, audit committee, legal department, etc.

b) Employees.

c) Specific cyber security roles, including.

1) Security Supervisor.

2) Cyber security internal auditor.

3) Security operators.

d) Personnel involved in network security level protection work, including.

1) The network security level protects work managers.

2) Network security level protection work implementation personnel.

3) Network security level protection work evaluation personnel.

7 Training content requirements

Financial institutions shall implement corresponding trainings in accordance with the requirements for implementing cyber security level protection for each post, including.

a) For full-staff training, the training content includes.

1) Network security awareness education.

2) Network security level protection policy document.

3) Network security laws, regulations and standards.

b) Conduct network security audit knowledge training for the audit committee.

c) Carry out training for safety supervisors, the training content includes.

1) Network security planning ability.

2) Knowledge of network security architecture.