

ICS 03.060
CCS A 11

JR

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

JR/T 0071.5-2020

**Implementation guidelines for classified protection of
cybersecurity of the financial industry - Part 5: Audit
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 Audit objectives
- 4 Auditor requirements
 - 4.1 Auditing principles
 - 4.2 Ability requirements
 - 4.3 Personnel training
 - 4.4 Personnel records
- 5 Audit information management requirements
 - 5.1 Confidentiality requirements
 - 5.2 Integrity requirements
- 6 Audit process requirements
 - 6.1 General
 - 6.2 Audit preparation

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 5 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 5: Audit requirements

1 Scope

This part stipulates the requirements for the implementation of auditing of the level of network security protection of financial institutions.

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

Protect audit 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 25058 Information Security Technology Network Security Level Protection Implementation Guide

3 Audit objectives

Through the network security grade protection audit, obtain relevant evidence of the financial institution's network security grade protection work, and conduct customer review on it.

To determine the level of network security protection in various financial institutions, such as rating, filing, construction rectification, self-examination, security inspection, etc.

Whether the requirements of network security level protection are followed in the work.

4.1 Auditing principles

Auditors should follow the following principles during the audit process.

- a) Ethical behavior. Auditors should be honest, upright and keep the secrets of the audited organization.
- b) Fair expression. Auditors should report the audit results truthfully and accurately.
- c) Professional competence. Auditors should have the necessary auditing competence.
- d) Independence. Auditors should be free of prejudice, have no conflicts of interest with the audited institution, and maintain an objective mind during the audit process.

To ensure that the audit findings and conclusions are only based on the audit evidence.

- e) Evidence-based. audit evidence should be based on available information samples.

4.2 Ability requirements

Auditors who implement graded protection audits for the financial industry should have the following capabilities.

- a) Familiar with the relevant policies and regulations of network security level protection.
- b) Correctly understand the network security level protection standard system and main standard content.

- c) Familiar with the whole process of grade protection work, including grading, filing, construction rectification, self-examination of evaluation, and safety inspection Requirements.
- d) Master the basic knowledge of network security, and be familiar with audit methods and procedures.
- e) Have the ability of comprehensive analysis and judgment, and be able to grasp the objectivity and accuracy of audit conclusions as a whole. Have strong textual expression ability.

4.3 Personnel training

Auditors who implement the cybersecurity level protection audit of the financial industry should participate in the organization of the financial industry cybersecurity level protection authority Relevant standard training to master the various requirements for the development of network security level protection in the financial industry.

4.4 Personnel records

Auditors should submit the latest records of their education, work experience, training and audit experience, as the audit agency to choose when arranging audit work.

The basis for selecting auditors.

5.1 Confidentiality requirements

Audit institutions are responsible for the confidentiality of information obtained during the audit process regarding the commercial, technical, and audit process of financial institutions.

Auditors should identify whether confidentiality is required for all information obtained or generated during the audit in accordance with the requirements of the audit agency. auditors and related personnel should not spread,, or leak confidential information in any form or excuse.

When the law requires confidential information to be provided to a third party, unless otherwise specified, the audit institution shall provide the information required by the law in advance.

Inform the financial institution of the information. When it is necessary to provide confidential information to other agencies (such as public security departments, confidential departments), the audit agency should take this action Inform the financial institution.

Audit institutions shall implement confidential management of information on audit activities, and configure and use corresponding security processing equipment and facilities as required. An Full processing equipment and facilities are mainly used for the establishment,