

ICS 03.060
CCS A 11

JR

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

JR/T 0071.3-2020

**Implementation guidelines for classified protection of
cybersecurity of the financial industry - Part 3: Post
competency requirements and guideline for evaluation
(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 Network Security Management Organizational Structure
4 Cybersecurity positions and responsibilities
5 Competence requirements for cybersecurity positions
6 Capability Evaluation of Cyber Security Personnel
References

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 3 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 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 3: Job Ability Requirements and Evaluation Guidelines

1 Scope

This part specifies requirements for the establishment of cyber security positions in financial institutions, requirements for cyber security job capabilities, and evaluation of cyber security personnel capabilities Claim.

This section is applicable to guide financial institutions to set up cyber security positions and develop cyber security job capabilities in accordance with the requirements of cyber security grade protection Requirements and implementation of network security personnel competency evaluation.

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 Network Security Management Organizational Structure

According to the requirements of GB/T 20269, GB/T 22239, GB/T 25058, GB/T 28448, the network security management organization structure is shown in Figure 1.

Show.

Figure 1 Network security management organization chart

4.1 Positions and responsibilities

Financial institutions' cybersecurity level protection work should follow relevant national standards and requirements, build a cybersecurity assurance system, and ensure that financial institutions Confidentiality, integrity and availability of information assets of the organization; responsibilities should be divided and assigned to corresponding positions to ensure that all important work is done in an effective manner.

Execute and complete.

Cybersecurity jobs involve two types of personnel.

- a) The original informatization staff who undertake the responsibility of network security.
- b) Individuals in specific cybersecurity positions set up separately for cybersecurity work.

4.2 Network Security Management Committee (Leading Group)

Financial institutions should establish a cyber security management committee composed of senior management, information technology departments and representatives of major business departments (Or known as the Information Security Leading Group).

The Cyber Security Management Committee shall be responsible for overseeing the implementation of various cyber security responsibilities, and regularly report to the board of directors and senior management of cyber security.

Implementation of the overall strategic plan, cyber security budget and actual expenditures, overall cyber security, etc. Specific responsibilities include but are not limited to the following Content.

- a) Review and approve the cyber security strategic plan of financial institutions.
- b) Make decisions on major issues related to network security, including network security organizational structure adjustments and major network security strategic changes Wait.
- c) Responsible for commanding and coordinating the handling of major cybersecurity

incidents in financial institutions.

- d) Responsible for communicating and coordinating major issues in cyber security work.
- e) Responsible for ensuring the funds, personnel, facilities and other resources required for the development of network security work.

4.3 Security Supervisor (Cyber Security Office)

Financial institutions should set up a security director (or set up a cyber security office, which can be located in the information technology department).

Security supervisors should have basic cybersecurity awareness, recognize the importance of cybersecurity work, and provide sufficient resources to support the financial for the smooth development of financial institutions' cybersecurity work, specific responsibilities include but are not limited to the following.

- a) Organize and implement the decisions made by the Cyber Security Management Committee on cyber security management.
- b) Responsible for organizing the establishment, implementation and daily operation of the network security assurance system.
- c) Responsible for specific coordination and communication on matters related to cyber security work.
- d) Responsible for the implementation and implementation of network security work, supervise and guide the development of network security work of various departments, and regularly report to network security the management committee reports.

4.4 Security Administrator

Information technology departments of financial institutions should set up security administrators to be responsible for the formulation and implementation of various network security management strategies of financial institutions.

Body responsibilities include but are not limited to the following.

- a) Organize the formulation of various network security management strategies and supervise their implementation.
- b) Responsible for the selection, deployment and maintenance of security systems such as anti-virus and intrusion detection.
- c) Responsible for the response and handling of network security incidents.
- d) Organize the formulation of cybersecurity emergency plans, and organize regular drills.
- e) Regularly organize personnel safety awareness training.