

ICS 35.240.40
CCS A 11

JR

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

JR/T 0197-2020

**Financial data security - Guidelines for data security
classification**

(English Translation)

Issued on: September 23, 2020

Implemented on: September 23, 2020

Issued by: People's Bank of China

Table of Contents

Foreword...	3
Introduction...	4
1 Scope...	5
2 Normative references...	5
3 Terms and definitions...	5
4 Objectives, principles and scope...	8
5 Data security grading...	10
6 Identification of important data...	21
Appendix A (Informative) Reference rules for data grading...	22
Appendix B (Informative) Changes in data security level...	79
Appendix C (Informative) Important data...	80
References...	82

1 Scope

This standard gives the objectives, principles and scope of financial data security classification, as well as the elements, rules and classification process of data security classification.

This standard applies to financial institutions to carry out electronic data security classification work; provides a reference for third-party evaluation agencies and other organizations to carry out data security inspection and evaluation.

2 Normative references

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are applicable to this standard.

GB/T 4754-2017 Industrial classification for national economic activities

GB/T 5271.1-2000 Information technology - Vocabulary - Part 1.

Fundamental terms

GB/T 25069-2010 Information security technology - Glossary

GB/Z 28828-2012 Information security technology - Guideline for personal information

protection within information system for public and commercial services

GB/T 35273-2020 Information security technology - Personal information security specification

JR/T 0158-2018 Data classification guidelines for securities and futures industry

JR/T 0171-2020 Personal financial information protection technical specification

3 Terms and definitions

The terms and definitions as defined in GB/T 25069-2010 and GB/T 35273-2017 as well as the following terms and definitions apply to this document.

3.1

Information

Knowledge about objects (such as facts, events, things, processes or thoughts, including concepts), which has a specific meaning in certain situations.

Note: Rewrite GB/T 5271.1-2000, definition 2.01.01.01.

3.2

Data

The reinterpretable formal representation of information, to be suitable for communication, interpretation or processing.

Note: It can be processed by manual or automatic means.

[GB/T 5271.1-2000, definition 2.01.01.02]

3.3

Privacy

The authority that an individual has to control or influence information related to, which involves who collects and stores it, who discloses it.

[GB/T 25069-2010, definition 2.1.63]

3.4

Information processing

System execution of information operations, including data processing, which can also include operations such as data communications and office automation.

3.5

Data processing

System execution of data manipulation.

Examples. Mathematical operations or logical operations of data, data merging or classification, program assembly or compilation, or text operations, such as editing, classification, merging, storage, retrieval, display or printing.

4.1 Data security grading goals

Data security grading aims to comprehensively sort out data assets and establish appropriate data security grade. It is a necessary prerequisite and basis for financial institutions to implement effective data grading management.

4.2 Principles of data security grading

Data security grading follows the following principles.

4.3 Scope of data security classification

In the process of financial data security grading, non-electronic financial data shall be implemented in accordance with relevant management regulations such as archives and documents; financial data involving state secrets shall be implemented in accordance with relevant national laws and regulations, which is not within the scope of this standard. The data security classification of the securities industry can be implemented with reference to JR/T 0158-2018.

5.1.1 Overview

Security (confidentiality, integrity, availability) is an important reference attribute in information security risk assessment. The possible impact (such as possible harm, loss or potential risk, etc.) after data security is breached is an important basis for determining the data security level, which mainly considers the two elements of the affected object and the degree of impact.

5.1.3 Degree of influence

The degree of influence refers to the magnitude of the impact after the data security of financial institutions is damaged. From high to low, it is divided into serious damage, general damage, minor damage, no damage. The relevant description is as shown in Table 1, which can be used as the reference to judge the degree of influence. The degree of influence should be determined by comprehensively considering factors such as data type, data characteristics, data scale, combined with financial business attributes to determine the degree of influence after data security is breached, for example.

5.2.1 Security impact assessment

Security impact assessment should comprehensively consider factors such as data type, data content, data scale, data source, institutional functions,

5.3.2 General rules for grading

The general rules for the classification of financial data security levels include but are not limited to.

5.4.1 Organizational guarantee

Determine the highest decision-making organization for data security management; establish and clarify relevant departments (or organizations) and their responsibilities, including but not limited to.

5.4.2 System guarantee

Establish relevant systems for data classification work; clarify and implement relevant work requirements, including but not limited to.

6 Identification of important data

The identification and verification of important data carried by financial institutions should comply with the relevant regulations of the state and industry authorities. Please refer to Appendix C for the description of the nature and content of important data, which is only for reference when financial institutions carry out data security classification work.

.....