

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

JR/T 0200-2020

**Financial technology innovation risk monitoring regulations
(English Translation)**

Issued on: October 21, 2020

Implemented on: October 21, 2020

Issued by: People's Bank of China

Table of Contents

1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviations	1
5 Risk Monitoring Framework	2
6 Risk Monitoring Process	3
7 Implementation of Risk Monitoring	4
References	23

Foreword

This document starts from the provisions of GB/T 1.1-2020 "Guidelines for Standardization Work Part 1: Structure and Drafting Rules of Standardization Documents" grass.

This document was submitted by the People's Bank of China.

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

Drafting organizations of this document. Department of Science and Technology of the People's Bank of China, Shanghai Headquarters of the People's Bank of China, Chengdu Branch of the People's Bank of China, Chinese CMBC Hangzhou Center Branch, China Payment and Settlement Association, China Internet Finance Association, Industrial and Commercial Bank of China Co., Ltd., China Agricultural Bank of China Co., Ltd., Bank of China Co., Ltd., China Construction Bank Co., Ltd., China Financial Electronics Corporation, Beijing Bank Union Gold Card Technology Co., Ltd., Beijing Zhongjin Guosheng Certification Co., Ltd., Beijing Financial Technology Industry Alliance, Bank of Communications Co., Ltd., China Life Property Insurance Co., Ltd., China CITIC Bank Co., Ltd., China Minsheng Bank Co., Ltd., China Merchants Bank Co., Ltd.

Co., Ltd., China Guangfa Bank Co., Ltd., Shanghai Pudong Development Bank Co., Ltd., Bohai Bank Co., Ltd., Bank of China Union Co., Ltd., Bank of Shanghai Co., Ltd., Bank of Chengdu Co., Ltd., Bank of Chongqing Co., Ltd., Bank of Suzhou Co., Ltd., Bank of Hangzhou Co., Ltd., Chongqing Rural Commercial Bank Co., Ltd., Shanghai Huarui Bank Co., Ltd., Shenzhen Qianhai WeBank Co., Ltd., Zhejiang Internet Commercial Bank Co., Ltd., Sichuan Xinwang Bank Co., Ltd., Transchem Payment Co., Ltd., Baixing Credit Information Co., Ltd., ICBC Technology Co., Ltd., CCB Financial Technology Co., Ltd., Industrial Digital Financial Services (Shanghai) Co., Ltd., Huawei Software Technology Co.,

Ltd., Tencent Cloud Computing (Beijing) Co., Ltd., Jingdong Digital Technology Holding Co., Ltd.

Co., Ltd., Du Xiaoman (Chongqing) Technology Co., Ltd., CICC Financial Certification Center Co., Ltd.

1 Scope

This document specifies the requirements for the risk monitoring of financial technology innovation applications, including the monitoring framework, process, and implementation.

This document is applicable to licensed financial institutions engaged in financial service innovation and related business systems, computing power storage, algorithm models, etc.

Technology companies that develop technology products are also applicable to related security assessment agencies, risk monitoring agencies, and self-regulatory organizations.

2 Normative references

The contents of the following documents constitute the indispensable clauses of this document through normative references in the text. Among them, dated quotations Only the version corresponding to that date is applicable to this document; for undated references, the latest version (including all amendments) is applicable Used in this document.

JR/T 0193-2020 Blockchain Technology Finance Application Evaluation Rules

3 Terms and definitions

The following terms and definitions apply to this document.

Fintech innovation institution Licensed financial institutions engaged in financial service innovation and research and development of technology products such as related business systems, computing power storage, algorithm models, etc.

Technology company.

Fintech innovation

Under the premise of complying with the requirements of current laws and regulations, departmental rules, and regulatory documents, in areas that do not yet have management rules, use New technology design, products or services for financial users.

Personal financial information Personal information acquired, processed, and stored by financial technology innovation institutions through the provision of financial services or technological products.

Note 1: Personal financial information in this document includes account information, identification information, financial transaction information, personal identification information, property

information, loan information, and Other information that reflects certain circumstances of specific individuals.

Note 2: Rewrite JR/T 0171-2020, definition 3.2.

4 Abbreviations

The following abbreviations apply to this document.

API. Application Programming Interface (Application Programming Interface) APP. Client Application Software (Application Software) DNS. Domain Name System (Domain Name System) IDS. intrusion detection system (intrusion detection system) QoS. Quality of Service (Quality of Service) RPO. Recovery Point Objective RTO. Recovery Time Objective TPS. Transactions Per Second WAF. Web Application Firewall (Web Application Firewall)

5.1 Overview

Financial technology innovation risk monitoring is mainly through data collection and correlation analysis of financial technology innovation applications, etc., to identify and discover possible Existing security incidents and risks are displayed and warned, to grasp the risk situation of financial technology applications, and to ensure the safety and stability of financial technology applications Operation to protect the legitimate rights and interests of consumers. The financial technology innovation risk monitoring framework is shown in Figure 1.

Figure 1 Risk monitoring framework for fintech application

5.2.1 Monitoring object

It mainly covers the business system, API, SDK, APP, etc. of financial technology innovation institutions (hereinafter referred to as innovation institutions).

5.2.2 Monitoring content

The monitoring content mainly includes personal financial information protection, financial transaction security, business continuity, service quality, technology use security, Internal control management, network security, complaints, public opinion, etc.

5.3.1 Principles of safety and control

Risk monitoring and prevention and control should be carried out in accordance with the principle of safety and control, to ensure that the risks of systems and services are controllable, and to respond to threats and risks in advance.

Plan for the disposal of risks.

5.3.2 Open sharing principle

According to the principle of open sharing, risk information reporting and risk data sharing should be carried out.

5.3.3 Privacy protection principle

In accordance with the principle of privacy protection, effective measures should be taken for the privacy information of individuals or financial transactions that may be involved in the risk monitoring process.

Security protection measures to ensure that private information is not leaked.

5.3.4 Principles of Disclosure and Supervision

In accordance with the principles of disclosure and supervision, actively disclose system and application risks, publish reports on a regular basis, actively accept supervision, and ensure that the system and the application runs safely.

6.1 Basic requirements

Innovative institutions shall accept the risk monitoring of monitoring institutions in accordance with this document, and conduct risk disposal in accordance with the requirements of regulatory agencies and self-regulatory organizations.

The monitoring process includes data collection, data analysis, risk warning, risk treatment, and information sharing.

During the risk monitoring process, all participants should take technical measures to ensure data security storage, access control, and sensitive information desensitization.

Data is safe throughout its entire life cycle.

6.2 Data collection

The monitoring organization shall classify the monitoring objects, clearly define the type, interface and communication method of data collection, and collect monitoring data for Data analysis provides source data, including.

- a) Unified data collection interface.
- b) Standardize the data.

6.3 Data analysis

The monitoring agency should clarify the analysis purpose and select the appropriate data analysis tool according to the technical and business risk prevention requirements of the