Chinastandards.org

ICS 03.060
CCS A11

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

chinastandards.org - PREVIEW

GB/T 42926-2023

Specification of financial information system cybersecurity risk assessment

金融信息系统网络安全风险评估规范

Issued on: August 6, 2023 **Implemented on: December 1, 2023**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Preview: page 1 of 4 shown, 62 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-42926-2023

Table of Contents

chinastandards.org · PREVIEW

Foreword

This document complies with the provisions of GB/T 1.1-2020 "Standardization Work Guidelines Part

1.Structure and Drafting Rules of Standardization Documents" Drafting. Please note that some content in this document may be subject to patents. The publisher of this document assumes no responsibility for identifying patents. This document is under the jurisdiction of the National Financial Standardization Technical Committee (SAC/TC180). This document was drafted by: China Financial Electronic Group Co., Ltd., Beijing National Financial Technology Certification Center Co., Ltd., Beijing Tianrong Information Network Security Technology Co., Ltd., Industrial and Commercial Bank of China Co., Ltd., AsiaInfo Technology (Chengdu) Co., Ltd. The main drafters of this document. Zhang Haiyan, Tang Hui, Gao Qiangyi, Pan Liyang, Zhang Lu, Zhang Shu, Yang Jian, Meng Xianzhe, Li Ji, Jin Hongyue, Li Zhelong.

As the integration of finance and technology becomes a new trend, new financial technology applications such as cloud computing, big data, Internet of Things, mobile Internet, and artificial intelligence have Application scenarios are growing explosively, and financial information systems are facing complex and ever-changing network security threats and an increasingly severe network security situation. Financial information system

Preview: page 2 of 4 shown, 62 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-42926-2023

network security risk assessment helps to comprehensively analyze the threats, vulnerabilities and risks faced by financial information systems, etc. level, and carry out risk treatment work based on the risk assessment results. In order to better adapt to the changes in financial technology, financial information system network security risks The risk assessment system also needs to be further improved. This document is based on mature risk assessment methodology, combined with the characteristics of financial information systems and the requirements for information system security construction. Network security risk assessment models, processes and risk analysis methods for financial businesses and financial information systems are common to financial information systems. Provide guidance on cybersecurity risk assessment. Specifications for Network Security Risk Assessment of Financial Information Systems

1 Scope

GB/T 42926-2023 specifies how cybersecurity risk is assessed in financial information systems. Risk assessment is where security spending is decided, and it is also the step most easily reduced to a spreadsheet whose numbers were chosen to justify a conclusion already reached. In finance the stakes make that unaffordable: the systems are interconnected, an incident at one institution propagates, and the regulator wants assessments from different institutions to be comparable - which they cannot be if each defines likelihood, impact and asset value in its own way. This document establishes the key points, the principles and the elements of risk assessment work, and specifies the requirements for each phase: the preparation stage, the identification stage, and the risk calculation and treatment stage. Fixing the phases and their outputs is what makes an assessment auditable, so that a reviewer can see what was identified, how it was valued and why a given risk was accepted rather than treated. It applies to cybersecurity risk assessment of financial information systems. Under ICS 03.060 and CCS A11, it is written for banks, insurers and payment institutions, for their internal audit and risk functions, and for the assessors and regulators who review their work.

This document establishes the key points, principles, elements and principles of risk assessment work, and stipulates the risk assessment preparation stage, identification stage, risk Requirements for calculation and processing phase work. This document is applicable to financial management departments, financial industry institutions and network security risk assessment service agencies when conducting financial information system network security. Complete risk assessment work.

Note. The "risk assessment" in the terms of this document refers to "financial information system network security risk assessment".

2 Normative reference documents

The contents of the following documents constitute essential provisions of this document

Preview: page 3 of 4 shown, 62 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-42926-2023

through normative references in the text. Among them, the dated quotations For undated referenced documents, only the version corresponding to that date applies to this document; for undated referenced documents, the latest version (including all amendments) applies to this document.

GB/T 20269-2006 Information security technology information system security management requirements

GB/T 20984-2022 Information security technology Information security risk assessment method

GB/T 22240-2020 Information security technology network security level protection grading guide

GB/T 25069-2022 Information security technical terms

GB/T 31509-2015 Information Security Technology Information Security Risk Assessment Implementation Guide

3 Terms and definitions

The following terms and definitions as defined in GB/T 20269-2006, GB/T 25069-2022 and GB/T 20984-2022 apply in this document.

3.1 asset value assetvalue An indication of the importance or sensitivity of an asset.

Note. Asset value is the attribute of the asset and is also the main content of asset identification.

4 Abbreviations

The following abbreviations apply to this document. ty)

Chinastandards.org · PREVIEW

Preview: page 4 of 4 shown, 62 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-42926-2023