ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 45577-2025

Data security technology - Risk assessment method for data security

数据安全技术 数据安全风险评估方法

Issued on: April 25, 2025 **Implemented on: November 1, 2025**

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

Table of Contents

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part 1: Structure and drafting rules for standardization documents" Drafting.

Please note that some of the contents of this document may involve patents. The issuing organization of this document does not assume the responsibility for identifying patents.

This document was proposed and coordinated by the National Cybersecurity Standardization Technical Committee (SAC/TC260).

This document was drafted by: China Electronics Technology Standardization Institute, National Information Technology Security Research Center, National Computer Network

Emergency Response Team Technical Processing Coordination Center, National Industrial Information Security Development Research Center, Central Cyberspace Affairs Office Data and Technology Support Center, China Information Security Evaluation Center, National Information Center, Information Engineering Institute of Chinese Academy of Sciences, Third Research Institute of Ministry of Public Security, Beijing Municipal Government Information Security Center Center, China Cybersecurity Review Certification and Market Supervision Big Data Center, University of Science and Technology of China, Institute of Software, Chinese Academy of Sciences, Alibaba Cloud Computing Co., Ltd., Beijing Kuaishou Technology Co., Ltd., Ant Technology Group Co., Ltd., and Huawei Technologies Co., Ltd.

The main drafters of this document are: Yang Jianjun, Yao Xiangzhen, Zhang Yuguang, Hu Ying, Chen Qi, Yang Tao, Lin Xingchen, Chen Te, Lu Lei, Lin Zhiqiang, Jiang Songhao, Shangguan Xiaoli, Ren Yingjie, Zhu Xuefeng, Yan Hui, Li Min, Zhao Ran, Liu Xize, Li Ye, Chen Jing, Xu Feng, Wang Hui, Wang Defu, Du Jing, Ma Ying, Zhang Yan, Su Yanfang, Li Yuan, Cheng Yuqi, Zuo Xiaodong, Zhang Liwu, Song Jing, Sun Yong, Wang Xin, Bai Xiaoyuan, Shao Meng, Sudan, Li Haidong, Zhang Mingtian, Gao Chentao.

Data security technology Data security risk assessment method

1 Scope

This document describes the basic concepts, element relationships, and analysis principles of data security risk assessment, and provides practical examples for data security risk assessment.

Implementation process, assessment content, analysis and evaluation methods, etc.

This document is applicable to guiding data processors and third-party assessment agencies in conducting data security risk assessments, and can also be used by relevant regulatory authorities.

For reference when implementing data security review assessments.

2 Normative references

GB/T 25069-2022

GB/T 43697-2024

3 Terms and definitions

The terms and definitions defined in GB/T 25069-2022 and the following apply to this document.

3.1 data

Any recording of information by electronic or other means.

3.2 Data security

By taking necessary measures, we ensure that data is effectively protected and legally used, and that there are mechanisms to ensure continuous security. ability.

3.3

Activities such as data collection, storage, use, processing, transmission, provision, disclosure, and deletion.

3.4 rationality

Data processing activities must comply with laws, administrative regulations, and common sense in cybersecurity and data security, and must not harm national security or public order.

The common interests and the legitimate rights and interests of individuals and organizations.

3.5

Threats, vulnerabilities, problems, hidden dangers that may lead to events that endanger the confidentiality, integrity, availability and reasonableness of data processing Suffering, etc.

Note. In this document, "risk sources" are referred to as such, which include risk sources that may lead to data security incidents due to security threats exploiting vulnerabilities, as well as data processing activities.