

ICS 35.240
CCS L 70



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

GB/T 46347-2025

Artificial intelligence - Risk management capability assessment

人工智能 风险管理能力评估

Issued on: October 5, 2025

Implemented on: October 5, 2025

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

Table of Contents

1.Scope	1
2 Normative References	1
3.Terms and Definitions	1
4.Artificial Intelligence Risk Management Capability Framework and Classification	2
4.1 Artificial Intelligence Risk Management Capability Framework	2
4.2 Artificial Intelligence Risk Management Process	3
4.3 Artificial Intelligence Risk Management Capability Level	4
4.4 Classification of Artificial Intelligence Risk Management Capabilities	5
4.5 Artificial Intelligence Risk Management Capability Item	6
5.Assessment of Artificial Intelligence Risk Management Capabilities	8
5.1 Assessment of Artificial Intelligence Risk Management Planning Capabilities	8
5.2 Assessment of Artificial Intelligence Risk Communication Capabilities	12
5.3 Assessment of Artificial Intelligence Risk Assessment Capabilities	13
5.4 Assessment of Artificial Intelligence Risk Management Capabilities	17
5.5 Assessment of Artificial Intelligence Risk Monitoring Capabilities	18
25 References	27

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 involve patents. The issuing organization of this document assumes no responsibility for identifying patents. This document was proposed and is under the jurisdiction of the National Information Technology Standardization Technical Committee (SAC/TC28). This document was drafted by: China Electronics Technology Standardization Institute, Institute of Software, Chinese Academy of Sciences, and Nanjing Software Technology Research Institute, Chinese Academy of Sciences. Shanghai SenseTime Technology Co., Ltd., China Construction Technology Group Co., Ltd., Beijing Mouyuan Consulting Co., Ltd., Shanghai Artificial Intelligence Industry Association Meeting, Hangzhou Half Universe Technology Co., Ltd., Peking University Wuhan Artificial Intelligence Research Institute, Hisense Group Holding Co., Ltd., Siemens (China) Co., Ltd., China Telecom Digital Technology Co., Ltd., Tongfang Knowledge Network Digital Publishing Technology Co., Ltd., Shanghai Computer Software Technology Co., Ltd.

Technology Development Center, Beijing Ruilai Smart Technology Co., Ltd., Shanghai Artificial Intelligence Research Institute, Beijing University of Aeronautics and Astronautics, iFlytek Co., Ltd. The company, Zhejiang Dahua Technology Co., Ltd., Beijing University of Posts and Telecommunications, China TravelSky Holding Company Limited, and Aviation Industry Corporation of China. Shenyang Aircraft Design Institute, Inspur Cloud Information Technology Co., Ltd., Chongqing Guoke Chuzhi Information Technology Co., Ltd., Inspur Software Technology Co., Ltd. The company, Shanghai Suiyuan Technology Co., Ltd., China Shipbuilding Group Corporation Comprehensive Technology and Economic Research Institute, University of Electronic Science and Technology of China, Beijing Aerospace... Tianjin Institute of Automatic Control, China Ordnance Industry Information Center, and Zhengzhou Apas Data Cloud Information Technology Co., Ltd. The main drafters of this document are. Fan Kefeng, Liu Zhangyu, Ye Heng, Dong Jian, Meng Lingzhong, Xu Yang, Ma Chenghao, Wu Geng, Zeng Tao, Fang Liang, and Rao Xue. Zhao Chunhao, Ma Shanshan, Wu Nianjing, Gu Lingyun, Fang Jing, Wu Qi, Xue Yunzhi, Gao Hui, Gao Feng, Chen Mingang, Chen Wenjie, Liu Chang, Hu Songzhi, Zhao Yuxia Chen Xi, Song Haitao, Liu Xianglong, Liu Aishan, Dong Qian, Yang Guang, Liu Junhua, Cheng Miao, He Zhaofeng, Weng Jialiang, Mei Ying, Zheng Jiajia, Zhu Xiaofang, Chen Liming Hao Liqiang, You Hongfeng, Wang Shining, Yang Tonghui, Wen Xiaoling, Wu Lijin, Li Zhaochuan, Wang Jinchao, Jiang Mengcen, Jiang Yan, Wu Huijia, Li Jinsong Yu Mingliang, Xie Minxi, Fan Zesen, Fu Wenlin, Deng Sai, Chen He, Yu Hongyun, Jiang Wei, Li Xiang, Zhang Tianyuan, Wang Shuanqi, Zhang Xu.

"Artificial intelligence risk management" is a broad concept that encompasses the management of all risks related to artificial intelligence, including but not limited to... Risks include technological risks (such as algorithmic bias and data leakage), ethical risks (such as algorithmic discrimination and ideological erosion), and application risks (such as system being compromised). Risks include hacking attacks, algorithms being used for deception, and legal risks (such as algorithm compliance and intellectual property infringement). This document primarily focuses on an organization's risk management capabilities when applying artificial intelligence systems. These risks may involve system stability, security, and other aspects. Risk management for artificial intelligence systems encompasses aspects such as security, performance, and compatibility with other systems. It aims to ensure the system operates as intended. This will help ensure that potential problems arise from system failures or vulnerabilities. The risk management process defined in this document is mainly based on the risk management process shown in Figure 1 of GB/T 24353-2022, and further elaborates upon it. This section incorporates the description of the artificial intelligence risk management process in ISO /IEC 23894 and considers the risks mentioned in the "Artificial Intelligence Safety Governance Framework". The document further details the activities that organizations should undertake and the capabilities they should possess when managing risks. Artificial Intelligence Risk Management Capability Assessment

1 Scope

GB/T 46347-2025 is the Chinese national standard covering grading an organisation on how well it manages AI risk - the governance and accountability, the identification of risks across the model lifecycle, the controls and the testing, the incident handling, and the maturity levels an assessment places it in. First edition, and it belongs with the multi-algorithm management standard GB/T 46351-2025. Already in force. Issued on 5 October 2025, it has been in force since 5 October 2025.

This document specifies the levels and requirements for an organization's artificial intelligence risk management capabilities, and describes the organization's artificial intelligence risk management capabilities. The evaluation method. This document is intended to guide assessors in evaluating an organization's capabilities in managing artificial intelligence risks.

2 Normative references

This document has no normative references.

3 Terms and Definitions

The following terms and definitions apply to this document.

3.1 Research and development of the mechanisms and applications of artificial intelligence systems. [Source: GB/T 41867-2022, 3.1.2]

3.2 An engineering system that produces outputs such as content, predictions, recommendations, or decisions for a given human-defined goal. Note

1.This engineering system uses a variety of artificial intelligence-related technologies and methods to develop models that represent data, knowledge, processes, etc., for the purpose of performing tasks. Note

2.Artificial intelligence systems have different levels of automation. [Source: GB/T 41867-2022, 3.1.8]

3.3 risk The impact of uncertainty on objectives. [Source: GB/T 23694-2024, 3.1.1]

3.4 Risk management To guide and control the organization's coordinated activities in terms of risk. [Source: GB/T 23694-2024, 3.2.1]

3.5 risk source Elements that, individually or in combination, may pose a risk. [Source: GB/T 23694-2024, 3.3.10]

3.6 capabilitydomain A collection of related processes within the risk management process framework.