

ICS 35.040
CCS L 80

JT

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

JT/T 1275-2019

**Security risk assessment guidance for transportation
information system**

交通运输信息系统安全风险评估指南 清晰版
(English Translation)

Issued on: January 1, 1970

Implemented on: October 1, 2019

Issued by: Ministry of Transport

Table of Contents

Foreword
1 Scope
2 Normative references
3 Terms and definitions
4 General requirements for risk assessment
4.1 Work organization
4.2 Implementation requirements
4.3 Implementation Principles
4.4 Implementation form
4.5 Implementation method
4.6 Risk assessment at various stages of the information system life cycle
5 Implementation of risk assessment
5.1 Evaluation Principle
5.2 Implementation process
5.3 Preparation for assessment
5.4 Asset Identification
5.5 Threat identification
5.6 Vulnerability identification
5.7 Risk analysis
5.8 Risk Management Plan
5.9 Risk assessment documents and records
Appendix A (Informative) Roles and Responsibilities of the Transport Information System Security Risk Assessment Implementation Team

Foreword

This standard is in accordance with GB/T Draft the rules given in 1-2009.

Please note that some elements of this document may involve patents. The issuer of this document is not responsible for identifying these patents.

This standard is proposed by and under the jurisdiction of the Technical Committee on Transportation, Information, Communications and Navigation Standardization.

This standard was drafted. China Communications and Information Center.

1 Scope

This standard specifies the general requirements and implementation requirements for security risk assessment of transportation information systems.

This standard applies to the assessment and management of security risks in transportation information systems.

2 Normative references

The following documents are essential for the application of this document. For dated references, only the dated version applies to this article Pieces. For undated references, the latest version (including all amendments) applies to this document.

GB/T 1984-2007 Information Security Technology Information Security Risk Assessment Specification

3 Terms and definitions

The terms and definitions defined in GB/T 1984 and the following apply to this document. For ease of use, GB/T is repeatedly listed below Some terms and definitions in 1984.

Asset asset

Information or resources that are valuable to the industry are the objects of security policy protection.

[GB/T 1984-2007, definition 3. 1] 3. 2 Asset value Characterization of the importance or sensitivity of an asset. Asset value is the property of assets content.

[GB/T 1984-2007, definition 3. 2] 3. 3 Availability Data or resource characteristics, authorized entities can access and use data or resources as required.

[GB/T 1984-2007, definition 3. 3] 3. 4 Confidentiality the characteristics of the data, which means that the data has not been provided or leaked to unauthorized individuals, processes or other entities degree.

[GB/T 1984-2007, definition 3. 5] 3. Five Integrity Features that guarantee that information and information systems will not be altered or destroyed without authorization. Including data integrity and system integrity.

[GB/T 1984-2007, definition 3. 10] JT/T 1275-2019 3. 6 Information security risk security risk Human or natural threats make use of vulnerabilities in information systems and their management systems to cause security incidents Into the impact.

[GB/T 1984-2007, definition 3. 6] 3. 7 Security risk assessment security assent According to relevant information security technology and management standards, the confidentiality

and completeness of information systems and the information processed, transmitted and stored by them the process of evaluating security attributes such as integrity and usability. It assesses threats to assets and threats the possibility of a security event, and the value of the assets involved in the security event to determine if a security event occurs to the industry influences.

[GB/T 1984-2007, definition 3. 7] 3. 8 Inspection and assessment assessment Initiated by the superior authority or business authority of the assessed industry, the information system and its Manage mandatory inspection activities.

[GB/T 1984-2007, definition 3. 9] 3. 9 Self-assessment Risk assessment of the information system and its management initiated by the owner of the information system, referring to relevant national regulations and standards activity.

[GB/T 1984-2007, definition 3. 13] 3. 10 Information security incident confidential information Caused by natural, man-made or software or hardware defects or failures, causing harm to information systems or negatively affecting society event.

[GB/T 1984-2007, definition 3. 14] 3. 11 Security measures safety Practices, regulations to protect assets, protect against threats, reduce vulnerability and reduce the impact of security incidents, and combat information crime Process and mechanism collectively.

[GB/T 1984-2007, definition 3. 15] 3. 12 Threat Causes of accidents that could cause harm to the system or organization.

3. 13

Vulnerability

Weakness of assets or certain assets that could be exploited.

[GB/T 1984-2007, definition 3. 18] 3. 14 Information system information system it is composed of computers and related and supporting equipment and facilities (including networks), and the information is imported according to certain application goals and rules.

Collection, processing, storage, transmission and retrieval systems.

JT/T 1275-2019

4 General requirements for risk assessment

4.1

Work organization the security risk assessment of transportation information systems should focus on self-assessment. Self-assessment and inspection and assessment should be combined and complement each other.

Development.

Self-assessment is initiated by the competent department of the information system, the operating unit or the user unit.

Information systems carry out risk assessments.

The inspection and evaluation work shall be carried out by the higher-level management department of the information system or the relevant national functional department according to law.

4.2

Implementation requirements the transportation information system security risk assessment should be carried out regularly by the competent department of the information system, the operating unit, and the using unit. in when major changes are made to the information system or operating environment (including the discovery of new major threats and vulnerabilities), or other emergence that may affect system security all conditions should be reopened. The risk assessment work carried out during the trial operation of the information system should be an important part of project acceptance content.

The results of the information system security risk assessment shall be recorded in the risk assessment report, and targeted security rectification recommendations shall be made.

The assessment situation and improvement measures are reported to the relevant network security supervision function.

4.3

Implementation principles the implementation of the security risk assessment of the transportation information system follows the following principles.

a) The principle of least impact. The stable operation of the information system should be guaranteed, and the evaluation and testing items that may cause impact should be selected in non-business Test during peak business hours or in a simulated environment.

b) the principle of controllability. All personnel involved in the assessment of the security service organization shall sign a confidentiality agreement.

According to strict management, it shall not be disclosed to any unit or individual without authorization; the evaluation tools used shall be obtained from the party being evaluated.

license.

c) the principle of objective fairness. The security service organization should collect evidence in the risk assessment to make an objective assessment of the security risks of the information system Fair judgment.

4.4

Implementation form the transportation information system security risk assessment can be carried out in the form of self-assessment or third-party assessment by security service