

ICS 03.100.01; 13.200
CCS A 90



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

GB/T 45157-2024

**Security and resilience - Community resilience - Guidelines for
information exchange between organizations**

安全与韧性 社区韧性 组织间信息交互指南

(English Translation)

Issued on: December 31, 2024

Implemented on: April 1, 2025

**Issued by: State Administration for Market Regulation, China National
Standardization Administration**

Table of Contents

Preface	
Introduction	
1 Scope	
2 Normative references	
3 Terms and Definitions	
4 Principle	
4.1 Overview	
4.2 Guiding Principles	
5 Frame	
5.1 Overview	
5.2 Leadership and Commitment	
5.3 Environmental Analysis	
5.4 Design and build framework	
5.5 Implementation	
5.6 Supervision and Review	
5.7 Continuous Improvement	
6 Process	
6.1 Overview	
6.2 Establishing Requirements	
6.3 Organizational Preparation	
6.4 Defining the information exchange structure	
6.5 Operation and maintenance information exchange	
6.6 Supervision and Review	
Appendix A (Informative) Traffic Light Protocol (TLP)	
Appendix B (Informative) Example	
B.1 Examples of cross-border information sharing in the energy sector	
B.2 Example of information sharing on community resilience projects	
Reference	

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.

This document is equivalent to ISO 22396:2020 "Guidelines for information exchange between organizations for secure and resilient communities".

The following minimal editorial changes were made to this document.

---Change the source of 3.1 from "ISO 22300:2018" to "ISO 22300:2021";

--- Deleted the expressions such as "private power companies" in Appendix B that do not conform to my country's national conditions;

--- Added "ISO/IEC 27000" to the references.

Introduction

The risk landscape has changed for all actors in society, including government agencies, enterprises, institutions, and other Organizations. Organizations are more interconnected and interdependent, leading to cross-domain and overlapping risks.

Key social infrastructure or services are gradually managed by various entities, which has a great impact on inter-organizational cooperation and information for capacity building.

The change in ownership patterns of key social infrastructure and services means that government agencies, enterprises, institutions and and other organizations need to be involved in developing mechanisms to increase response capacity, enhance experience and improve knowledge exchange.

While territorial governments have a duty to serve and protect their citizens, preventive measures to improve the safety of key social functions have traditionally been viewed as Government agencies and the public sector are at the core of the solution, but solutions often come from all parts of society.

To protect and support preventive protection measures, it is necessary for actors in government agencies, enterprises, institutions, and other organizations to exchange information efficiently and securely.

Generally speaking, the purpose of collaboration is to identify risks and initiate actions to improve security and reduce vulnerability.

The exchange of information about the responsibilities, threats, and vulnerabilities of organizations can improve the effectiveness and efficiency of organizational operations.

Establishing accurate information sharing boundaries between organizations is challenging

but necessary.

Different solutions are developed for different industries, regions or countries, so coordination responsibilities are difficult to determine.

Companies also need to ensure that their sensitive information will not be leaked, used to hinder competition or damage their business activities and brands.

Comprehensive information exchange is a necessary condition for successful and effective information exchange among government agencies, enterprises, institutions and other organizations.

Organizations that participate in information exchange can increase their knowledge and understanding of events and risks to strengthen resilience.

Such organizations bring other benefits, including.

- Provide guidance to organizations that may not be able to obtain access;
- Strengthen capabilities by opening up restricted information through other means;
- Create centralized information exchange to support sharing;
- Improve information distribution capabilities;
- Build organizational responsibility through caring and sharing.

This document is divided into three parts. principles, framework and process. Principles are the core content of this document, and the framework determines the information exchange.

The process describes the procedures for establishing and maintaining the information exchange. Figure 1 shows the relationship between principles, frameworks, and processes.

Figure 1 Relationship between principles, frameworks and processes

Safety and Resilience Community Resilience Guidelines for information exchange between organizations

1 Scope

This document provides guidance on information exchange between organizations and defines the principles, framework and process of information exchange so that participating organizations can benefit from their Learn from people's mistakes or successes and provide relevant measures to strengthen the organization's ability to deal with risks.

This document is intended for private and public organizations requiring guidance on establishing conditions to support the exchange of information.

This document does not apply to specific technical aspects and focuses mainly on

methodology.

Note: Legal regulations vary from jurisdiction to jurisdiction. It is the responsibility of the document user to determine the applicability of relevant legal regulations to this document.

2 Normative references

The contents of the following documents constitute the essential clauses of this document through normative references in this document.

For referenced documents without a date, only the version corresponding to that date applies to this document; for referenced documents without a date, the latest version (including all amendments) applies to this document.

Note: GB/T 44483-2024 Security and resilience terminology (ISO 22300:2021, MOD)

3 Terms and definitions

For the purpose of this document, the terms and definitions defined in ISO 22300 and listed below apply.

sensitive information Information that cannot be disclosed publicly because it could have an adverse impact on the organization, national security, or public safety.

[Source. ISO 22300:2021, 3.1.260, modified]

4.1 Overview

The overall goal of information exchange is to share information between trusted organizations as part of informed decision making to improve security and resilience.

The specific needs and resources of an organization make each information exchange unique, so at the initial stage, it is advisable to formulate appropriate principles to guide information interaction so that it can be effectively evaluated and continuously improved.

4.2 Guiding Principles

To effectively exchange information, participating organizations should follow the following guiding principles.

- a) Trust and willingness. Trust and willingness based on information exchange (including sensitive information).
- b) Create value. Create and protect the value of the organization based on mutual benefit.
- c) Information Protection. Information exchange requires a mutual understanding of sensitive information designated by each participating organization.
- d) Structured and systematic processes. Organizations follow information policies,