INTERNATIONAL STANDARD

ISO 22396

First edition
2020-02

Security and resilience — Community resilience — Guidelines for information exchange between organizations

Sécurité et résilience — Résilience des communautés — Lignes directrices pour l'échange d'informations entre les organismes

Reference number
ISO 22396:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The landscape of risk has changed for all actors in society, including private enterprises, governmental organizations and non-governmental organizations. Organizations have become more interconnected and interdependent, resulting in risks that overlap and cross boundaries.

Changing ownership patterns of critical societal infrastructure and services mean that private enterprises must be involved in the development of mechanisms for increased coping capacity, experience and knowledge exchange. Critical societal infrastructure or services are increasingly privately managed or owned, creating new requirements for co-operation and information exchange for capacity building purposes.

While the authorities having jurisdiction have the ultimate responsibility to serve and protect their citizens, solutions are often found in the private sector, even though preventive measures for the increased security of critical societal functions have traditionally been regarded as government and public core areas. In order to enhance and support preventive measures for protection, multiple actors from both the private and public sectors should be able to exchange information effectively and securely in order to increase societal security and enhance resilience.

Generally, the objective of collaboration is to identify and initiate actions to increase security and reduce vulnerability. Information exchange on possible liabilities, risks and vulnerabilities can enhance the effectiveness and efficiency of organizations.

It is challenging but necessary to establish accurate boundaries between organizations regarding information sharing. Responsibility for coordination is also difficult to define since coordination in these areas requires special solutions adapted within a sector, for each different sector, region or nation.

Private actors also require a guarantee that their sensitive business information is not leaked, used to impede competition or to damage their business and trademark. Consequently, secure information exchange is an essential condition of successful and effective information exchange for both public and private organizations.

Organizations that participate in information exchange arrangements can increase their knowledge and understanding of events and risks with the aim of enhancing resilience. Effective information exchange arrangements can provide other benefits to these participating organizations, including:

— enlightening organizations that may not usually get access in usual ways;

— enhancing capabilities by unlocking otherwise restricted information;

— creating a centralized information exchange to support sharing;

— increasing capacity for information distribution;

— creating a sense of community through caring and sharing.

This document is divided into three segments: principles, framework and process. The principles present the core of this document. The framework identifies the necessary elements for developing information exchange frameworks. The process describes information exchange procedures for establishing and maintaining the arrangement. Figure 1 presents the relationship between the principles, the framework and the process.

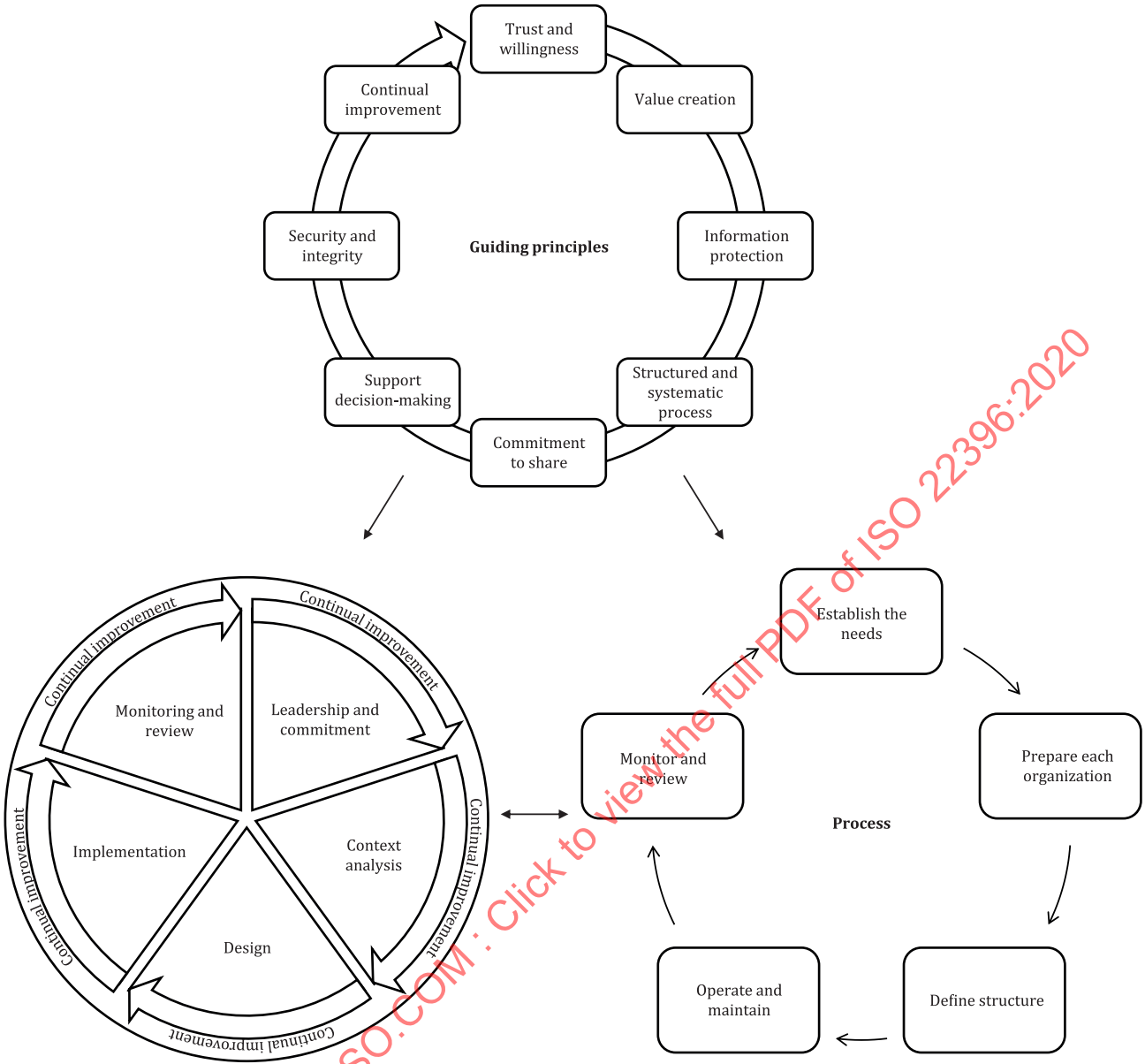

Figure 1 — Relationship between principles, framework and process

Security and resilience — Community resilience — Guidelines for information exchange between organizations

1 Scope

This document gives guidelines for information exchange. It includes principles, a framework and a process for information exchange. It identifies mechanisms for information exchange that allow a participating organization to learn from others' experiences, mistakes and successes. It can be used to guide the maintenance of the information exchange arrangement in order to increase commitment and engagement. It provides measures that enhance the ability of participating organizations to cope with disruption risk.

This document is applicable to private and public organizations that require guidance on establishing the conditions to support information exchange.

This document does not apply to technical aspects but focuses on methodology issues.

NOTE Legislation can differ from jurisdiction to jurisdiction. It is the user's responsibility to determine how applicable legal requirements relate to this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22300, *Security and resilience — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
sensitive information
information that is protected from public disclosure only because it would have an adverse effect on an individual, organization, national security or public safety

[SOURCE: ISO 22300:2018, 3.244, modified — "individual" has been added.]

4 Principles

4.1 General

The overall goal of any information exchange arrangement is to share information between trusted organizations as part of informed decision-making to increase security and enhance resilience (see Annex B for examples). While each exchange arrangement will be unique, based on the specific needs

and resources of these participating organizations, common principles should guide the exchange arrangement and guide the exchange's evaluation and continuing improvement, from the outset.

4.2 Guiding principles

In order for information exchange to be effective, participating organizations should apply the following guiding principles.

a) **Trust and willingness**

Information exchange is based on trust and the willingness to exchange information, including sensitive information.

b) **Value creation**

Information exchange creates and protects the values of participating organizations and is founded on mutual benefit.

c) **Information protection**

Information exchange requires a mutual understanding of sensitive information as specified by each participating organization.

d) **Structured and systematic process**

Organizations sharing information do so within the context of information policies, procedures and practice, relevant legislation and privacy principles and it is carried out within a systematic, timely and structured framework.

e) **Commitment to share**

Information exchange is based on a commitment to give and receive information to ensure mutually beneficial relationships.

f) **Support decision-making**

Information exchange is used to help make decisions and guide day-to-day operations.

g) **Security and integrity**

Credible and effective security and integrity controls enable effective information exchange arrangements.

h) **Continual improvement**

Participating organizations are committed to regular assessments to identify opportunities for the continual improvement of information exchange.

5 Framework

5.1 General

The framework ensures effective information exchange to inform sense, meaning and decision-making for the participating organizations.

Figure 2 describes the components of the framework for establishing and maintaining information exchange arrangements.

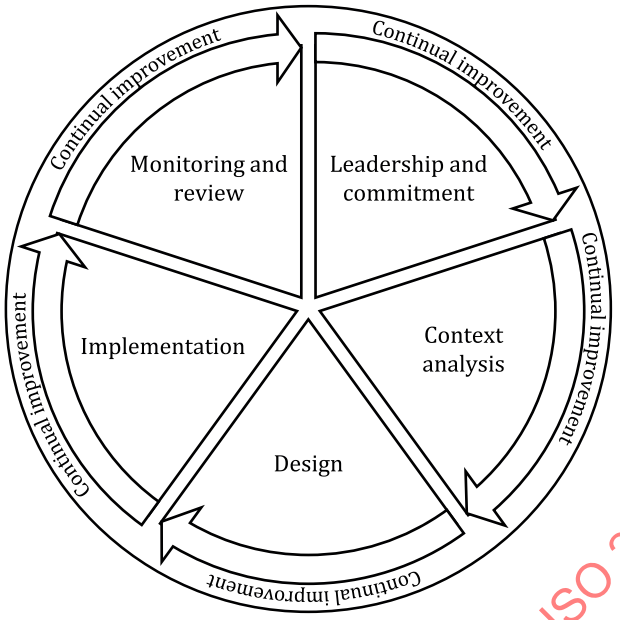

Figure 2 — The framework components

5.2 Leadership and commitment

Top management should demonstrate a strong and sustained commitment to ensure the ongoing effectiveness of the information exchange arrangement, adapting the components of the framework and supporting the arrangement to the extent necessary to ensure its effective implementation.

Top management should:

— define objectives for the information exchange in the value creation process;

— define and endorse an information exchange framework;

— ensure organizational commitment and contribution;

— assign accountabilities and responsibilities for participation;

— ensure that necessary resources are allocated to the information exchange arrangement;

— communicate the benefits from sharing information within the arrangement;

— determine performance criteria for information exchange that are aligned with the interests and context of the participating organizations;

— ensure compliance with their organization's policies;

— develop a policy document incorporating these commitments.

5.3 Context analysis

Before designing and implementing a framework for information exchange, the participating organizations should evaluate and understand the external and internal context that will influence the design.

Assessing the participating organizations' external context may include:

— the context in which they operate;

— key drivers and trends that impact the context;

— relationships with their stakeholders.

Assessing the participating organizations' internal context may include:

— identifying which parts of each organization are to participate;

— identifying the representatives of each organization to be part of the process.

5.4 Designing and establishing a framework

When designing a framework for information exchange, the top management of the participating organizations should consider:

— the governance model, organizational structure, roles, accountabilities and principles for information dissemination;

— the resource capabilities and knowledge that are required (e.g. capital, time, staff, expertise);

— formal and informal decision-making processes;

— relationships with, and perceptions and values of, internal stakeholders;

— the organizational culture.

5.5 Implementation

When implementing the framework, the participating organizations should:

— communicate and consult with stakeholders to ensure that the framework remains appropriate;

— ensure that decision-making, including the development and setting of objectives, is aligned with the outcomes of the information exchange arrangement.

5.6 Monitoring and review

In order to ensure that the information exchange is effective and continues to support organizational performance, the participating organizations should:

— assess the performance and progress of the established objectives for the information exchange;

— review the documentation for the information exchange process (e.g. the risk management plan);

— review the framework;

— review the balance of contributions of the participating organizations.

The participating organizations should provide a supportive role to other participating organizations in the monitoring and review process.

5.7 Continual improvement

The participating organizations should use the outcomes of the monitoring and review process to continuously improve the information exchange framework.

Lessons learned should be documented and shared among the participating organizations.

6 Process

6.1 General

Figure 3 presents an overview of the information exchange process.

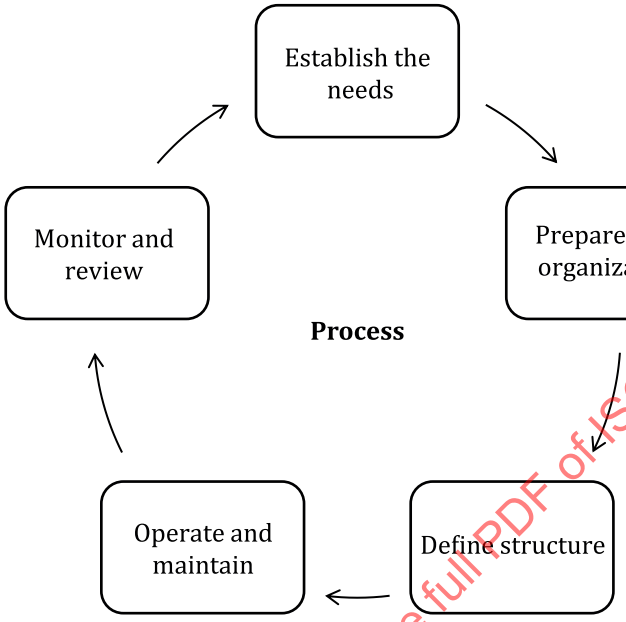

Figure 3 — Overview of the information exchange process

The participating organizations should:

— establish and operate information exchange arrangements as a mechanism that allows each organization to learn from others' inputs, successes, mistakes and experiences;

— embed the information exchange arrangements in each organization's general operational processes;

— customize and optimize the information exchange arrangement to each organization's local requirements and environment;

— ensure that the information exchanged is subject to a process that ensures the security of the information.

6.2 Establish the needs

6.2.1 General

The participating organizations should:

— set the structure for the information exchange;

— articulate the objectives and clarify the parameters for the information exchange;

— identify opportunities to express opinions and to influence the information exchange process;

— scrutinize the information exchange process to confirm that each organization can relate to the scope and function of the framework;

— build trust among the participating organizations by ensuring the proper use of methods and techniques.

6.2.2 Expression of interest

An organization should indicate their interest in participating in the information exchange arrangement by a letter of intent or other means of committing to the information exchange.

6.3 Prepare each organization

6.3.1 Internal

The participating organizations should develop a policy and procedures for the information sharing arrangement that considers:

— the type of information that is exchangeable;

— the type of information that will be of value when obtained;

— the information that would be of value to other participating organizations.

6.3.2 External

The participating organizations should establish processes and protocols for handling information that has been shared in the information exchange arrangement in order to determine:

— the sensitivity of the information;

— the value of the information when exchanged;

— how they can respond to this information with additional important information.

6.4 Define the information exchange structure

6.4.1 General

The participating organizations should agree upon the information exchange structure, provide an overview of the information exchange, including a governance process and a code of conduct, and specify how the information exchange is to be funded.

6.4.2 Purpose

The participating organizations should clarify the purpose of the information exchange by explaining how each organization relates to the information exchange arrangement and by specifying:

— the general processes for contributing information within the information exchange arrangement;

— the practical aspects for the exchange of information;

— the type of information that is required;

— ways in which they can provide input or thoughts on the information exchanged.

6.4.3 Membership guidelines

The participating organizations should establish guidelines for participation in the information exchange arrangement, including, for example:

— an overview of the purpose and objectives of the information exchange arrangement;

— how to resolve confidentiality issues;

— administrative matters;

— descriptions and clarifications of any specific purposes;

— the frequency and type of meetings;

— specifications on any financial commitments;

— specifications on any legal commitments;

— authority specifications for all the participating organizations;

— how the participating organizations' membership list is managed;

— how a chair for the information exchange is appointed;

— guidelines for the dissemination of information.

6.4.4 Information classification system

An information security management system should be an integrated part of the information exchange structure. Security aspects should be taken into account in the structuring of processes, systems and controls. An information security management system should include several controls on information assets.

As a first step in the process of establishing the information exchange, the participating organizations should create and agree upon a classification scheme for the information, taking into consideration how the information exchange arrangement will relate to already established protocols and concepts. The classification of information should be made in accordance with value, criticality and sensitivity to unauthorized disclosure or modification. Legal requirements can apply. The classification should indicate the value of the asset in terms of confidentiality, integrity and availability, and should be continuously updated throughout the whole life cycle.

The classification of information is an exclusive decision of the organization (private or public) owning the information and is decided based on operational concerns and/or the sensitivity of information.

Examples of information classification systems include the following.

— Information security management systems (see the ISO/IEC 27000 family of standards): such a framework protects the confidentiality of the information, as well as its correctness and availability by managing risks and bringing trust to the involved parties.

— The traffic light protocol (TLP): the information classification system TLP is meant to encourage greater sharing of sensitive information between organizations. It allows the source of information to tag it with a colour, specifying to the recipient the terms of further distribution or disclosure. If a wider distribution than what the coding permits is required, the recipient must first consult the source who has the last word. The TLP requires a certain trust amongst the participators. The sharer must trust the receivers enough to not over-tag the information, and the receivers must trust the sharer's reasons for tagging it with a certain colour and respect those limitations. (See Annex A.)

6.5 Operate and maintain the information exchange

6.5.1 General

The participating organizations should have established routines and processes for how to run and maintain the information exchange arrangement, including processes for developing and obtaining technical assistance and updating it as required.

The participating organizations should encourage face-to-face meetings and agree to a platform for sharing information in order to make the information exchange effective and efficient.

6.5.2 Meetings

The participating organizations should consider the following points when creating a functional information exchange:

— the frequency of meetings;

— different types of meetings;

— attendance requirements;

— obligations for personal participation (e.g. substitutes not permitted);

— expectations for personal trust among participants;

— information sharing at closed meetings;

— agreed meeting conditions;

— co-chairs of the private and public organizations;

— practical activities in working groups;

— rules for inviting guests to meetings.

6.5.3 Information sharing platform

The participating organizations should consider how the sharing platform can be used for information exchange outside of face-to-face meetings.

6.5.4 Technical aspects

The participating organizations should choose a suitable technical platform and make decisions with respect to the different technical aspects of the information exchange, ranging from security aspects of the meeting rooms to secure communication that can be used for information exchange when not attending meetings.

The platform should be chosen to recognize that trustful information sharing is highly dependent on appropriate procedures, so that sensitive information is anonymized and only distributed in a proper format. The technical aspects of the information exchange should be under continual development and include best practices that increase the level of security.

NOTE This document does not specify technical requirements but identifies principles for using technical support in information exchange.

6.6 Monitoring and review

6.6.1 General

The participating organizations should include requirements for monitoring and review of the information exchange as part of the planned process for regular (ad hoc or periodic) checking or surveillance. Responsibilities for monitoring and review should be clearly defined. The monitoring and review process should encompass all aspects of the risk management process so that it:

— ensures that controls are effective and efficient in both design and operation;

— obtains further information to improve the information exchange;

— analyses and considers learning lessons from activities (including near-misses), changes, trends, successes and failures;

— detects changes in the external and internal context;

— identifies emerging risks affecting efficiency.

6.6.2 Continual improvement

The participating organizations should continually improve the effectiveness of the information exchange, recognizing that continual improvement:

— operates at all levels within the Plan-Do-Check-Act (PDCA) model;

— should be driven by evaluation, monitoring and analysis of monitored events, corrective actions and management review;

— requires a process that properly identifies problems and nonconformities and then fixes them.

The continual improvement process should:

— address the nature of the problem and the environment within which the problem exists;

— include changing the environment to ensure that the problem does not recur;

— include steps that build and improve on the previous step so that improvement covers more aspects than just the original identified problem and has a wider, more sustainable effect on the organization;

— follow the same basic process as used for corrective actions and include the following:

  — identify what to address and the present condition (nonconformity);

  — identify the present process and controls (root cause);

  — determine what changes to implement (corrective action).

The participating organizations should implement corrective actions to address deficiencies in the information exchange to ensure that it functions as intended and takes the information exchange to a higher level of efficiency and effectiveness.

Annex A
(informative)

Traffic light protocol (TLP)

The traffic light protocol (TLP) is a set of designations used to ensure that sensitive information is shared with the correct audience. It employs four colours to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s), as explained in Table A.1.

Table A.1 — Traffic light protocol

Colour	Meaning
TLP:RED	The information is strictly limited to named recipients only. The recipients are not allowed to share the information with any third parties. Example: One-to-one, informing people in a meeting or via direct email.
TLP:AMBER	The distribution is limited to the recipient's organizations on a need-to-know basis. The source is allowed (and expected) to further specify distributive limits that the recipient must adhere to. Example: One-to-some, exclusively given to an organization to be acted upon.
TLP:GREEN	The distribution is limited to a particular community. The recipient may not, however, release the information outside of the community or share it through publicly accessible channels. Example: One-to-many, information to a community or a group of organizations.
TLP:WHITE	The distribution of the information is unlimited, although subject to standard copyright rules. Example: One-to-any, publicly shared information.

SOURCE: Reference [9], modified.