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.

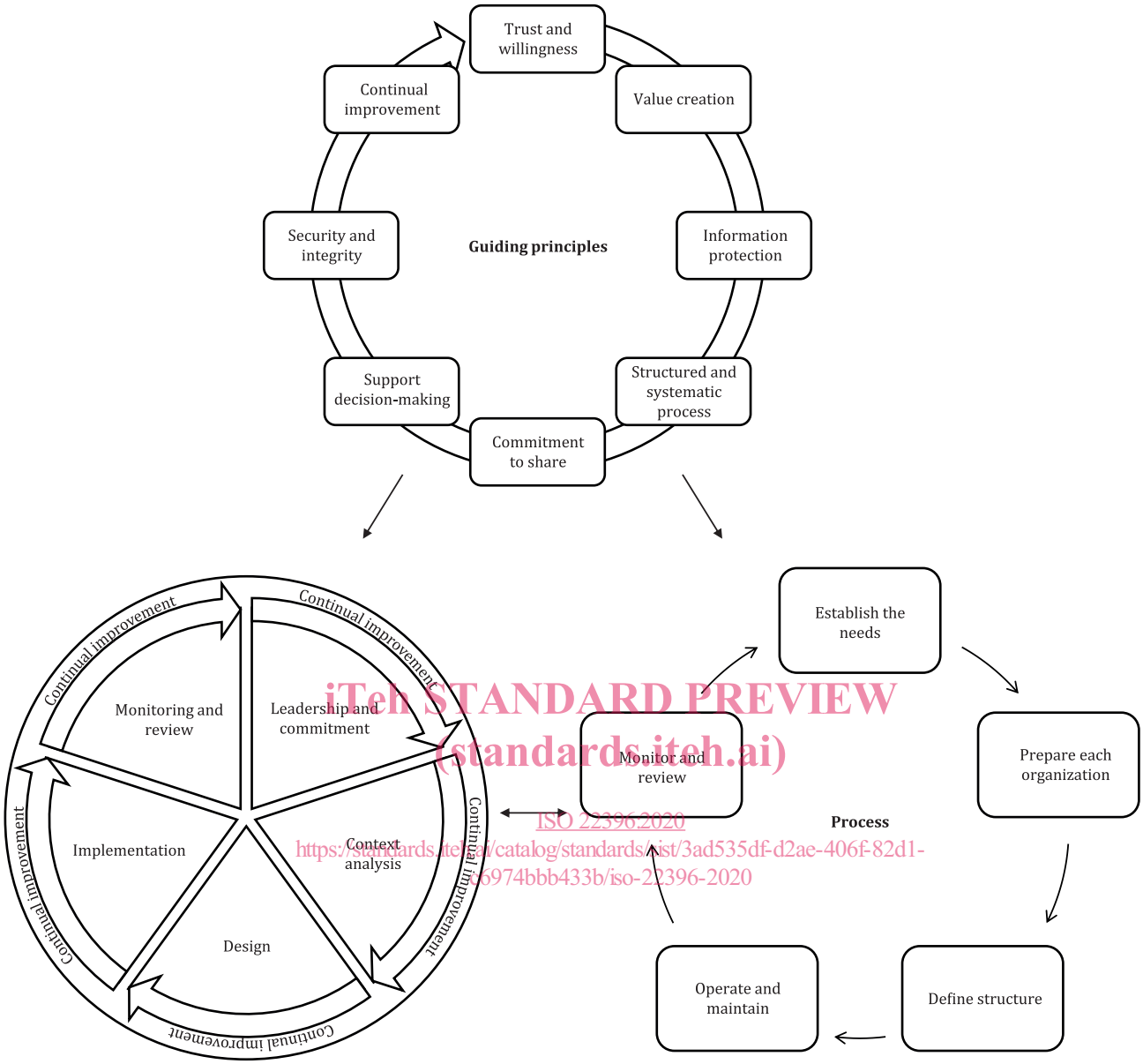

Figure 1 — Relationship between principles, framework and process

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.

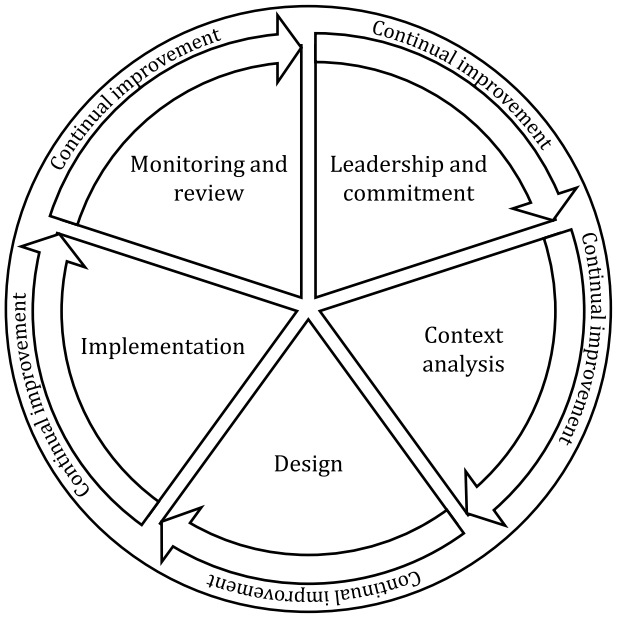

Figure 2 — The framework components

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.

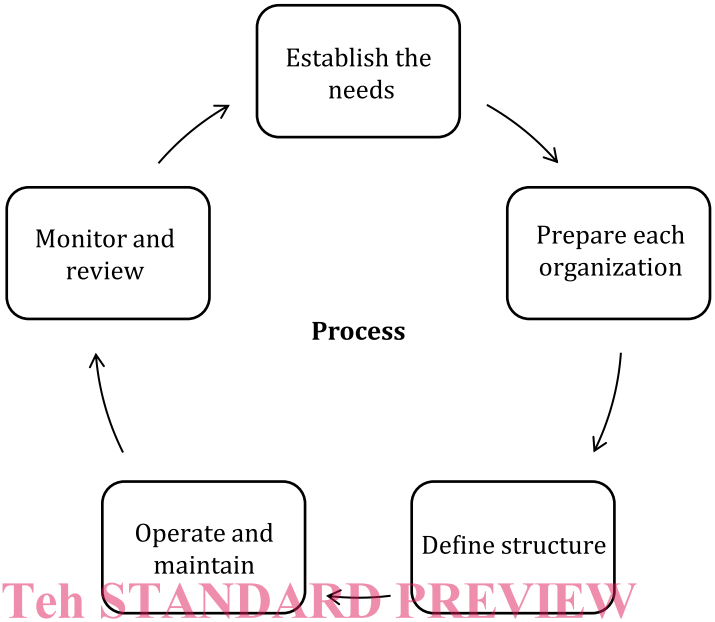

Figure 3 — Overview of the information exchange process

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.