



BSI Standards Publication

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

National foreword

This British Standard is the UK implementation of [ISO 22396:2020](#).

The UK participation in its preparation was entrusted to Technical Committee SSM/1, Societal security management.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2020
Published by BSI Standards Limited 2020

ISBN 978 0 580 93423 0

ICS 03.100.01

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 29 February 2020.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

INTERNATIONAL STANDARD

ISO
22396

First edition
2020-02-10

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)
Documents
Document Sharing Hub
© ISO 2020



COPYRIGHT PROTECTED DOCUMENT

© ISO 2020, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Principles	1
4.1 General	1
4.2 Guiding principles	2
5 Framework	2
5.1 General	2
5.2 Leadership and commitment	3
5.3 Context analysis	3
5.4 Designing and establishing a framework	4
5.5 Implementation	4
5.6 Monitoring and review	4
5.7 Continual improvement	4
6 Process	5
6.1 General	5
6.2 Establish the needs	5
6.2.1 General	5
6.2.2 Expression of interest	6
6.3 Prepare each organization	6
6.3.1 Internal	6
6.3.2 External	6
6.4 Define the information exchange structure	6
6.4.1 General	6
6.4.2 Purpose	6
6.4.3 Membership guidelines	6
6.4.4 Information classification system	7
6.5 Operate and maintain the information exchange	7
6.5.1 General	7
6.5.2 Meetings	8
6.5.3 Information sharing platform	8
6.5.4 Technical aspects	8
6.6 Monitoring and review	8
6.6.1 General	8
6.6.2 Continual improvement	9
Annex A (informative) Traffic light protocol (TLP)	10
Annex B (informative) Examples	11
Bibliography	13

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.