



BSI Standards Publication

**Security and resilience — Authenticity, integrity
and trust for products and documents —
Guidelines to establish and monitor a
protection plan and its implementation**

National foreword

This British Standard is the UK implementation of [ISO 22384:2020](#).

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 committee manager.

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 0 539 00242 3

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 31 October 2020.

Amendments/corrigenda issued since publication

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

INTERNATIONAL STANDARD

ISO
22384

First edition
2020-10-26

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines to establish and monitor a protection plan and its implementation

*Sécurité et résilience — Authenticité, intégrité et confiance pour les
produits et les documents — Lignes directrices pour l'établissement et
la surveillance d'un plan de prévention et sa mise en œuvre*



Reference number
ISO 22384:2020(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 General	2
5 Generic procedure model	2
5.1 Establish project team.....	2
5.2 Identify assets to protect.....	3
5.3 Define protection objectives.....	3
5.4 Perform risk assessment.....	4
5.5 Specify selection criteria for protection measures.....	4
5.6 Select appropriate measures.....	5
5.7 Combine and reconcile measures for protection plan.....	7
5.8 Specify protection plan and prepare implementation.....	7
5.9 Validate protection plan.....	7
5.10 Implement protection plan.....	8
5.11 Evaluate effectiveness of deployed protection plan.....	8
5.12 Maintain protection plan.....	9
Annex A (informative) Common product-related threats and risks	10
Annex B (informative) Product life cycle view	13
Annex C (informative) Supply chain view	15
Bibliography	16

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

Due to the increasing level of interconnection of the global economy and the growing availability of complex manufacturing processes as well as globalized trade relations, there is a growing motivation and ability for counterfeiting, unfair trade and other product-related threats. This is shown, for example, by the continually growing number of product confiscations related to brand piracy and counterfeiting. To become more resilient, manufacturers have to introduce organizational and technical measures as part of a protection plan to withstand physical or digital attacks and other product-related threats.

In order to introduce protection measures in a precise and effective way, organizations should implement a systematic evaluation process for the selection of appropriate organizational, technical and legal measures, depending on the respective threat. Protection measures offered on the market can represent only a partial solution.

For an effective and long-term protection, a reasonable and systematic combination of individual measures, and their proper evaluation and implementation is necessary. The procedure can be represented as a Plan-Do-Check-Act (PDCA) cycle, see [Figure 1](#).

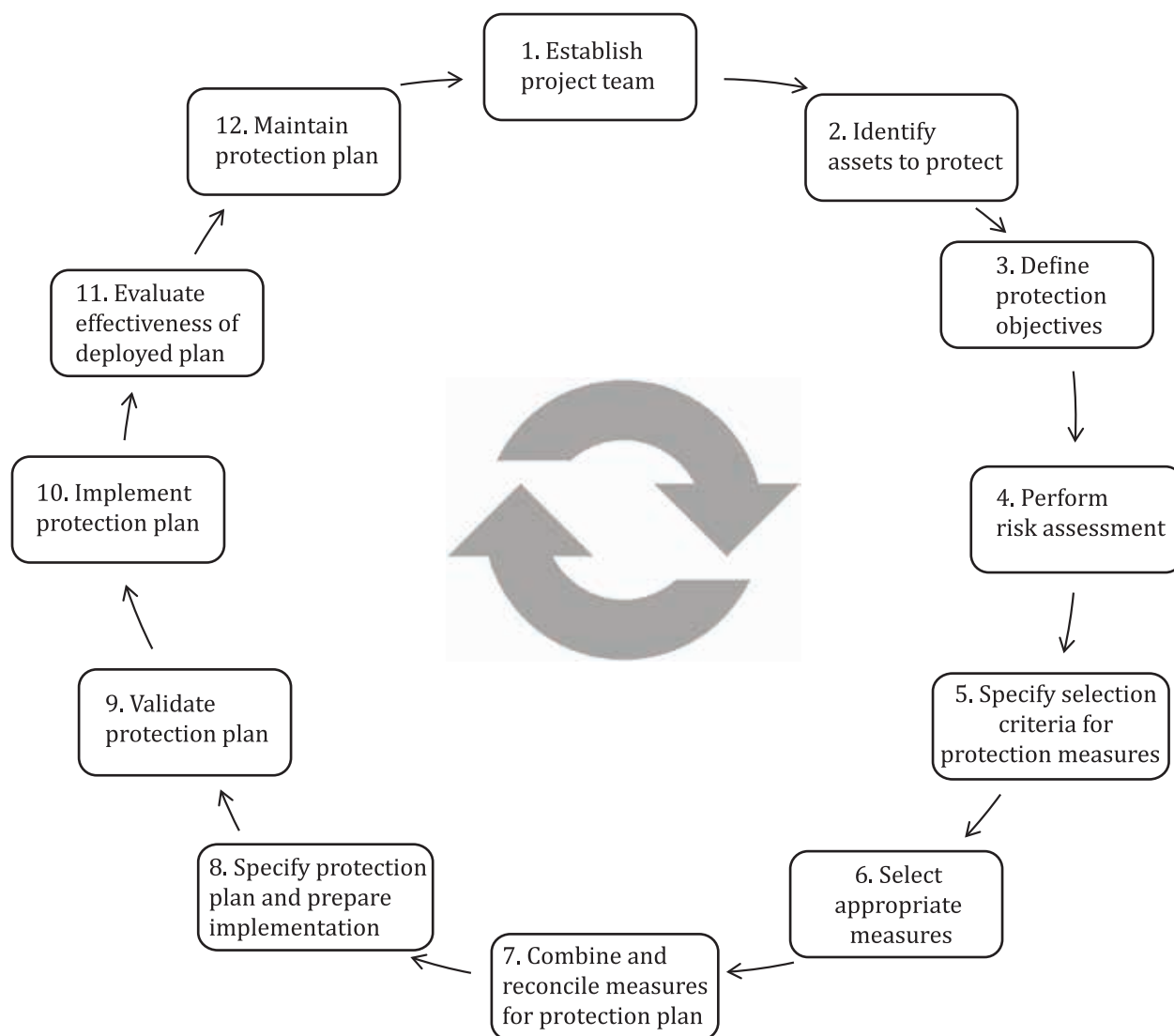


Figure 1 — Generic procedure model for the implementation of a protection plan (PDCA)

Product-related threats affect rights owners, manufacturers, distributors, service providers and consumers in many ways. The potential damage of such threats includes:

- loss of innovation leadership;
- decreased sales;
- damage to reputation or brand equity;
- loss of jobs;
- tax losses;
- danger to the health and safety of consumers;
- environmental issues.