INTERNATIONAL STANDARD

ISO 22384

First edition
2020-10

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)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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

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.

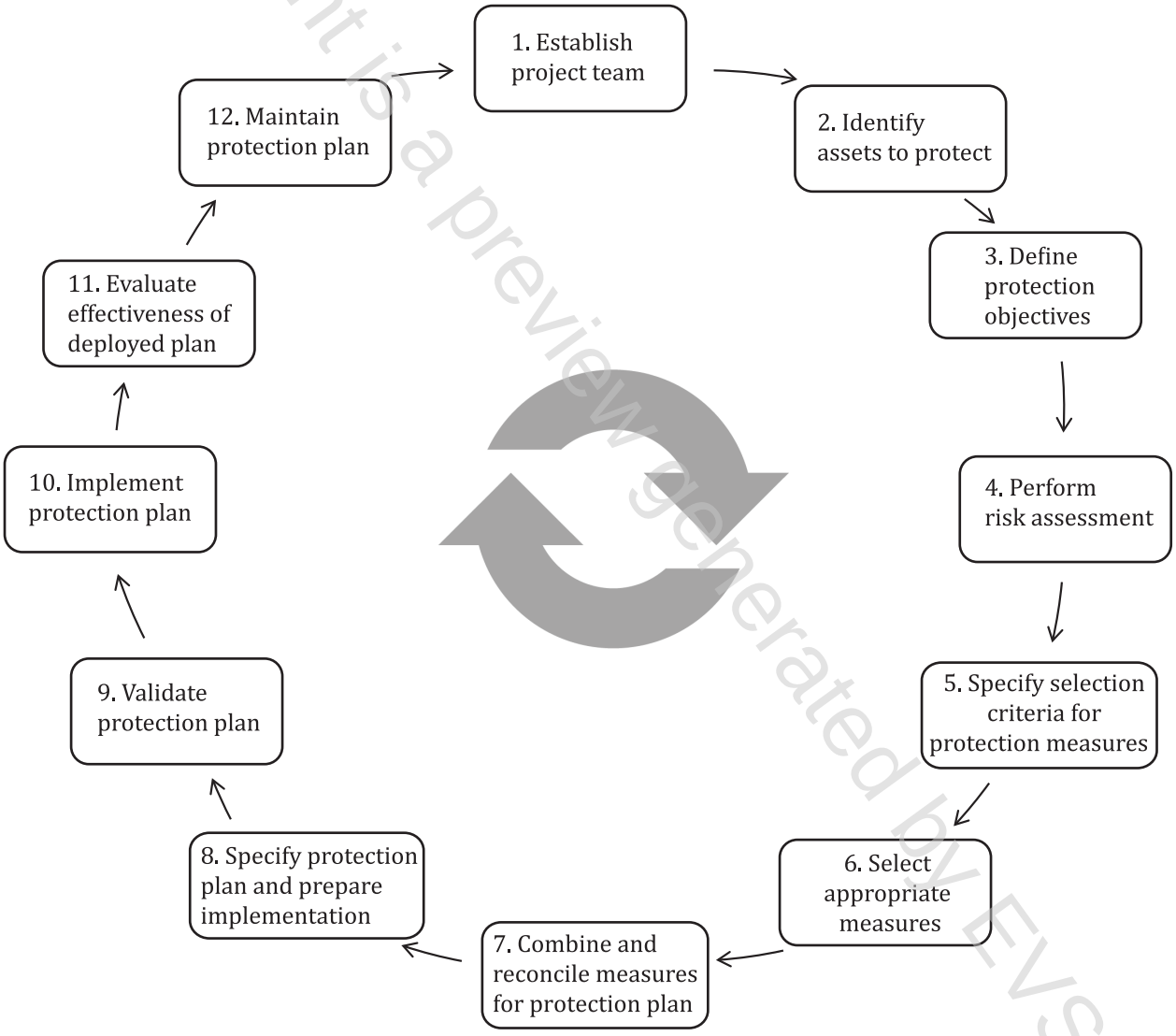

Figure 1 — Generic procedure model for the implementation of a protection plan (PDCA)

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.

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

1 Scope

This document gives guidelines for assessing product security-related threats, risks and countermeasures by developing a suitable protection plan, supporting its implementation and monitoring its effectiveness after implementation.

This includes consideration of impacts and modifications to, for example, product life cycle, supply chain, manufacturing, data management, brand perception and costs so as to adapt the protection plan accordingly.

This document is applicable to all types and sizes of organizations that want to ensure authenticity and integrity in order to support the trustworthiness of products, including documents, data and services related to products.

This document supports organizations setting up a process to assess risks and to select and combine individual measures for developing a product protection plan.

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
brand
intangible asset, including but not limited to, names, terms, signs, symbols, logos and designs, or a combination of these, intended to identify goods, services or entities, or a combination of these, creating distinctive images and associations in the minds of stakeholders, thereby generating economic benefit/values

[SOURCE: ISO 20671:2019, 3.1]

3.2
brand piracy
use of a *brand* (3.1) without the brand owner's permission