TECHNICAL SPECIFICATION

ISO/IEC TS 27110

First edition
2021-02

Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines

Sécurité de l'information, cybersécurité et protection de la vie privée — Lignes directrices relatives à l'élaboration d'un cadre en matière de cybersécurité

Reference number
ISO/IEC TS 27110:2021(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) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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 document 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 and IEC 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) or the IEC list of patent declarations received (see patents.iec.ch).

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 Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

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

Cybersecurity is a pressing issue due to the use of connected technologies. Cyber threats are continually evolving, thus protecting users and organizations is a constant challenge. To cope with this challenge, business groups, government agencies, and other organizations produce documents and tools called cybersecurity frameworks to help organize and communicate cybersecurity activities of organizations. These organizations producing the cybersecurity frameworks are referred to as "cybersecurity framework creators." Other organizations and individuals then use or reference the cybersecurity framework in their cybersecurity activities.

Given that there are multiple cybersecurity framework creators, there are a multitude of cybersecurity frameworks. The current set of cybersecurity frameworks is diverse and varied. Organizations using cybersecurity frameworks are challenged with harmonizing different lexicons and conceptual structures to meet their requirements. These cybersecurity frameworks then become competing interests for finite resources. The additional effort could be better spent implementing cybersecurity and combating threats.

The goal of this document is to ensure a minimum set of concepts are used to define cybersecurity frameworks to help ease the burden of cybersecurity framework creators and cybersecurity framework users.

As this document limits itself with a minimum set of concepts, its length is kept to a minimum on purpose. This document is not intended to supersede or replace the requirements of an ISMS given in ISO/IEC 27001.

The principles of this document are as follows:

- flexible — to allow for multiple types of cybersecurity frameworks to exist;
- compatible — to allow for multiple cybersecurity frameworks to align; and
- interoperable — to allow for multiple uses of a cybersecurity framework to be valid.

The audience of this document is cybersecurity framework creators.

Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines

1 Scope

This document specifies guidelines for developing a cybersecurity framework. It is applicable to cybersecurity framework creators regardless of their organizations' type, size or nature.

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/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC TS 27100, *Information technology — Cybersecurity — Overview and concepts*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC TS 27100 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
cybersecurity framework
basic set of concepts used to organize and communicate cybersecurity activities

3.2
cyber persona
digital representation of an individual or organization necessary to interact in cyberspace

[SOURCE: U.S. DoD Joint Publication 3-12 and Caire, J, & Conchon, S:2016]

3.3
asset
anything that has value to an individual, an organization or a government

[SOURCE: ISO/IEC 27032:2012, 4.6, modified — The Note has been removed.]

4 Overview

Cybersecurity framework creators face a unique challenge: create a framework which is general enough to allow for flexibility in use while providing a structure to allow for compatibility and interoperability across frameworks and uses. Striking a balance between flexibility and compatibility while satisfying stakeholder requirements can be difficult. Developing multiple cybersecurity frameworks using the