TECHNICAL SPECIFICATION

ISO/IEC TS 27100

First edition
2020-12

Information technology — Cybersecurity — Overview and concepts

Reference number
ISO/IEC TS 27100:2020(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) 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 broad term used differently through the world.

Cybersecurity concerns managing information security risks when information is in digital form in computers, storage and networks. Many of the information security controls, methods, and techniques can be applied to manage cyber risks.

ISO/IEC 27001 provides requirements for information security management systems. The focus of ISO/IEC 27001 is on security of information, and associated risks, within environments predominantly under the control of a particular organization. Cybersecurity focuses on the risks in cyberspace, an interconnected digital environment that can extend across organizational boundaries, and in which entities share information, interact digitally and have responsibility to respond to cybersecurity incidents.

Information technology — Cybersecurity — Overview and concepts

1 Scope

This document provides an overview of cybersecurity.

This document:

- describes cybersecurity and relevant concepts, including how it is related to and different from information security;
- establishes the context of cybersecurity;
- does not cover all terms and definitions applicable to cybersecurity; and
- does not limit other standards in defining new cybersecurity-related terms for use.

This document is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations).

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 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
cyber attack
attack
malicious attempts to exploit vulnerabilities in information systems or physical systems in *cyberspace* (3.5) and to damage, disrupt or gain unauthorized access to these systems

Note 1 to entry: Expression of an offensive operation in or through the cyberspace leading to unauthorized use of services, creating illicit services, orchestrating denial of service, altering or deleting data or resources.

3.2
cybersecurity
safeguarding of people, society, organizations and nations from cyber *risks* (3.7)

Note 1 to entry: Safeguarding means to keep cyber risks at a tolerable level.