TECHNICAL SPECIFICATION

ISO/IEC TS 27100

First edition

Information technology — Cybersecurity — Overview and concepts

PROOF/ÉPREUVE

Reference number
ISO/IEC TS 27100:2020(E)

COPYRIGHT PROTECTED DOCUMENT

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.

 PROOF/ÉPREUVE

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.

3.3
cybersecurity event
occurrence indicating a possible breach of *cybersecurity* (3.2) or failure of controls

[SOURCE: ISO/IEC 27035-1:2016, 3.3, modified — In the term and the definition, “information security” has been replaced with “cybersecurity”.]

3.4
cybersecurity incident
one or multiple related and identified *cybersecurity events* (3.3) that can harm people, society, organizations or nations

[SOURCE: ISO/IEC 27035-1:2016, 3.4, modified — In the term and the definition, “information security” has been replaced with “cybersecurity”. In the definition, new wording has been added after "harm".]

3.5
cyberspace
interconnected digital environment of networks, services, systems, people, processes, organizations, and that which resides on the digital environment or traverses through it

Note 1 to entry: Interconnected digital environment that traverses public infrastructure e.g. the internet, rather than parts of the organisation’s internal network or air-gapped digital environments that may not traverse public infrastructure.

[SOURCE: ISO/IEC 27102:2019, 3.6, modified — In the definition, the part after "processes" has been added.]

3.6
cyber threat
potential cause of an unwanted *cybersecurity incident* (3.4), which can result in harm to a system, people, society, organization, or other entities in *cyberspace* (3.5)

[SOURCE: ISO/IEC 27000:2018, 3.74, modified — The term “threat” has been replaced with “cyber threat”. In the definition, “incident” has been replaced with “cybersecurity incident”, and new wording has been added after "system".]

3.7
risk
effect of uncertainty on objectives

Note 1 to entry: Cyber risk can be expressed as effect of uncertainty on objectives of entities in *cyberspace* (3.5).

Note 2 to entry: Cyber risk is associated with the potential that threats will exploit vulnerabilities in cyberspace and thereby cause harm to entities in cyberspace.

[SOURCE: ISO/IEC 27000:2018, 3.61, modified — Notes 1 to 6 to entry have been replaced.]

4 Concepts

4.1 Cyberspace

Cyberspace is a complex environment based on digital technologies that provides a global place for digital interaction among people including formal and informal interactions with public or private entities such as businesses, governments, non-profit organizations and other groups. Cyberspace is public but as individual components of cyberspace are owned by a variety of entities, it can be considered both public and private space. People and entities interact in cyberspace for many different purposes. This interaction is manifested as sharing, exchange, processing or receipt of information.

Any interaction taken in cyberspace by an individual or an entity potentially has a near-instantaneous impact anywhere in the world.

While interactive actions in cyberspace create knowledge and power, the following features of cyberspace can bring both advantageous and adverse consequences:

a) cyberspace is borderless;

b) anyone can enter and leave cyberspace freely or at a very low cost;

c) cyber actors can be anonymous or obfuscated; and

d) a threat agent can be anywhere in cyberspace from the opposite side of the globe to a close neighbour of the target.

An action in cyberspace and its impacts can be asymmetric. The originating action can have consequences disproportionate in difficulty and cost of counteraction. In order to take advantage of cyberspace, it is important to prevent adverse consequences, that is, to ensure cybersecurity.

4.2 Cybersecurity

The objective of adequate cybersecurity is to maintain an acceptable level of stability, continuity and safety of entities operating in cyberspace. While it is not possible to always achieve these objectives, cybersecurity aims to reduce cyber risks to a tolerable level.

Areas of concern for cybersecurity include:

a) stability and continuity of society, organizations and nations;

b) property (including information) of people and organizations; and

c) human lives and health.

Cybersecurity with these characteristics is implemented by individual organizations. In cyberspace, organizations need to consider not only themselves, but also other parties who share cyberspace. While an organization needs to manage its vulnerabilities to ensure that the organization does not adversely affect other actors, it needs to work with others to reduce cyber risks. In addition, cybersecurity needs to reduce social and human losses in real space caused by cybersecurity incidents in cyberspace. Therefore, immediate detection and appropriate response of information security incidents are important elements of cybersecurity.

5 Relationship between cybersecurity and relevant concepts

5.1 Relationship between information security and cybersecurity

Information security and cybersecurity have different perspectives and concerns while they are closely related and overlapping.

Information security is defined in ISO/IEC 27000 as “preservation of confidentiality, integrity and availability of information”. It primarily deals with information. The definition is general, does not specify its application and subject entity. Once an entity with its context is determined as subject of information security, concerns of information security can be established, e.g.;

a) confidentiality of information that has value to an organization;

b) integrity and availability of information that is critical to business operation;

c) availability of information and communication technology (ICT) infrastructure on which business processes depend; and

d) reliable and trusted delivery of ICT services.

Breach of information security in cyberspace can cause a cybersecurity incident. This means that the information security risks are viewed as cyber risks in the context of cybersecurity. However,

cybersecurity and information security differ in their objectives. Cybersecurity is primarily concerned about protecting entities including people, society, organizations and nations from cyber risks (see 4.2), while information security addresses to maintaining confidentiality, integrity and availability of information with consequences.

Cyberspace can contain information systems controlling physical devices and systems. Compromising information security of these connected information systems via the cyberspace can have implications on society or individuals. Cybersecurity reduces the likelihood of such events.

In order to reduce social, human and economic impacts caused by cybersecurity incidents, entities who connect to cyberspace have a responsibility for collectively managing cyber risks including sharing information about cyber risks, implementing protective controls, monitoring and detecting potential incidents, and cooperating in response and recovery from incidents. Activities of information security are performed by an entity that handles the information to reduce its own risks. However, cybersecurity is performed by an entity to address not only its own risks, but also risks of the other entities that are directly or indirectly involved. Those entities can reside anywhere in cyberspace.

5.2 Relationship between ISMS and cybersecurity

5.2.1 Cyberspace as a field of risk sources for an ISMS

An information security management system (ISMS) is applicable within an organization with interfaces and interactions with external entities. Specifically, the scope of the ISMS and the scope of risk identification are within an organization [see ISO/IEC 27001:2013, 4.3 and 6.1.2 c)]. Information security objectives (see ISO/IEC 27001:2013, 6.2) aim at protection of information that has value to the organization or of the information of other entities that are in custody of the organization.

Cybersecurity transcends the boundaries and control of an organization because of the interconnectedness of cyberspace. Organizations frequently interface and interact with external entities by using cyberspace. As such, the use of cyberspace represents risks to the organization that need to be managed as a part of an organization's ISMS. If the organization has an ISMS, cyberspace shapes part of context of the ISMS as referred to in ISO/IEC 27001:2013, 4.1. Threat vectors that originate in cyberspace can expose the organization to information security risks. The organization identifies risks from threats in cyberspace, along with other risks, during the process of risk identification as required in ISO/IEC 27001:2013, 6.1.2 c).

5.2.2 ISMS in support of cybersecurity

An ISMS provides a mechanism for organizations to use a risk-based, prioritized, flexible and communications-enabling approach to manage information security risks based on its business needs. An organization can operate its ISMS as a means of managing cyber risks. This is facilitated by a consistent and iterative approach to identifying, assessing and managing risk and evaluating implementation of the ISMS. An ISMS as described in ISO/IEC 27001 is applicable regardless of an organization's size and should also reflect a clear understanding of the organization's particular business drivers and security considerations. An ISMS facilitates communication about the implementation of these desired outcomes and associated information security activities across the organization, from the top management level by the management system requirements, to the implementation and operations levels by the controls. The application of ISMS does not only provide a clear and understandable set of controls as an outcome but also provide a clear scope of the cybersecurity activities in the organization and where boundaries and dependencies are.

An example of using an ISMS in support of cybersecurity is the use of ISO/IEC 27001 with ISO/IEC 27019 to establish, implement, maintain and continually improve an ISMS for the energy utility supplier. The ISMS supports the stability of the energy supply and, hence, contributes to the cybersecurity of a nation.

