ISO/IEC 27032

Search

Search this site

ISO/IEC 27032:2023 — Cybersecurity — **Guidelines for Internet security** *(second edition)*

Abstract

"[ISO/IEC 27032] provides:

- *an explanation of the relationship between Internet security, web security, network security and cybersecurity;*
- *an overview of Internet security;*
- *identification of interested parties and a description of their roles in Internet security;*
- *high-level guidance for addressing common Internet security issues.*

[The standard] is intended for organizations that use the Internet."

[Source: ISO/IEC 27032:2023]

Introduction

ISO/IEC 27032 addresses Internet security *i.e. "protecting Internet-related services and related ICT systems and networks as an extension of network security".*

Scope and purpose

The abstract above covers the scope and purpose.

The introduction notes that *"[ISO/IEC 27032] does not specifically address controls that organizations can require for systems supporting critical infrastructure or national security. However, most of the controls mentioned*

ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039
ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27046
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27090
ISO/IEC 27091
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27109
ISO/IEC TS 27110
ISO/IEC TS 27115
ISO/IEC 27116
ISO/IEC 27400
ISO/IEC 27402
ISO/IEC 27403
ISO/IEC 27404
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC 27557
ISO/IEC 27559
ISO/IEC TS 27560

in [ISO/IEC 27032] can be applied to such systems." In other words it *primarily* concerns the ordinary everyday network security threats facing all Internet users, particularly businesses rather than the more extreme spooky threats of concern in the governmental and defence domain.

Structure and content

The five main sections are:

5. Relationship between Internet security, web security, network security and cybersecurity.
6. Overview of Internet security.
7. Interested parties.
8. Internet security risk assessment and treatment.
9. Security guidelines for the Internet.

   Annex A. Cross-references between this standard and ISO/IEC 27002.

The annex cites a reasonable assortment of 50 controls from ISO/IEC 27002:2022

- 25 Organizational controls;
- 2 People controls;
- 0 Physical controls; and
- 23 Technological controls.

Status of the standard

The *first* edition was published in **2012**.

The *second*, thoroughly revised edition was published in **2023**.

Personal comments

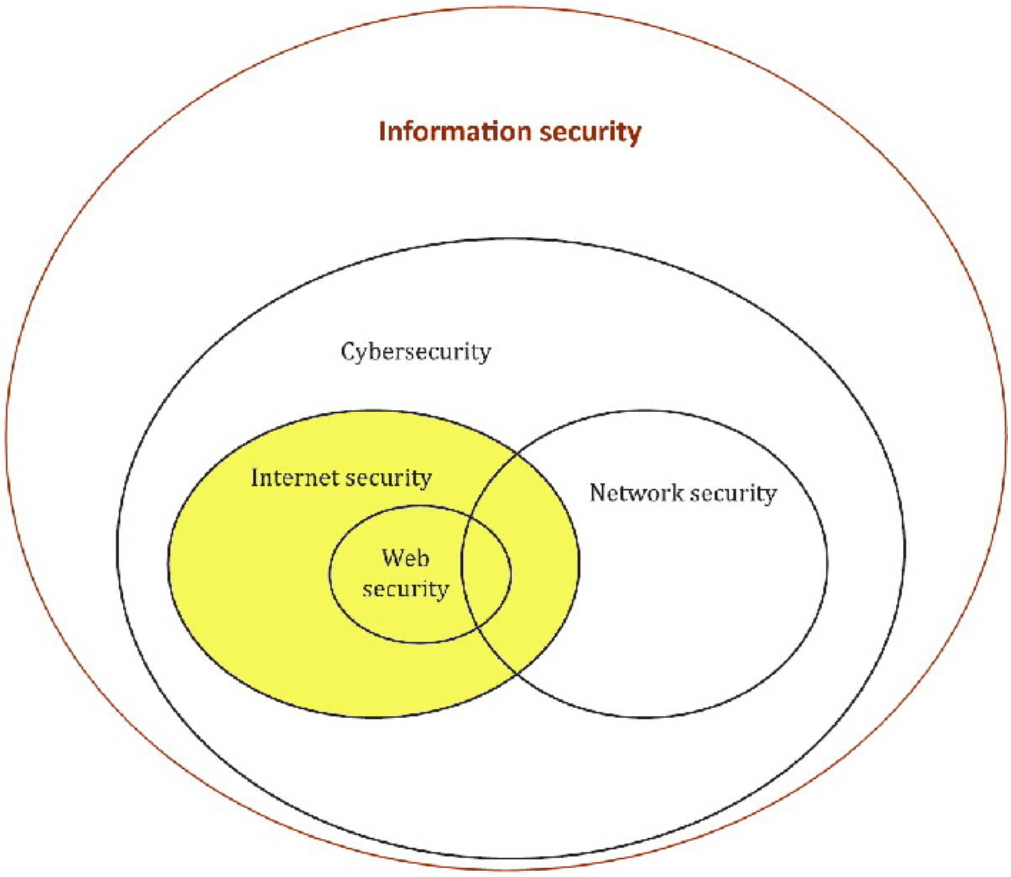
See also ISO/IEC 27100.

Over the last decade or so, "cyber" as in "cybersecurity" has gradually become a buzzier buzzword and yet doubts and disagreements over what it actually means persists. SC 27 had the *opportunity* to clarify cyber-related terms when revising this standard but the second edition simply reproduces the definition of cybersecurity from ISO/IEC TS 27100:2020 *vis "safeguarding of people, society, organizations and nations from cyber risks Note 1 to entry: Safeguarding means to keep cyber risk at a tolerable level."* ... but fails to define "cyber risk", failing yet again to clarify what it is that we are supposedly being safeguarded against. Other cyber terms defined in the first edition have simply been dropped.

Meanwhile, the second edition remains myopically focused on deliberate attacks perpetrated via the Internet by hackers, malware, phishers and spammers.

I've taken the liberty of elaborating on the scope diagram from the standard, highlighting in yellow the coverage area and adding an outer circle for the field of information security as a whole:

ISO/IEC 27561
ISO/IEC 27562
ISO/IEC TR 27563
ISO/IEC 27564
ISO/IEC 27565
ISO/IEC 27566
ISO/IEC 27568
ISO/IEC 27569
ISO/IEC TS 27570
ISO/IEC 27573
ISO/IEC 27701
ISO/IEC 27706
ISO 27799



< Previous standard ^ Up a level ^ Next standard >