DS information

DS/ISO/IEC TS 27100:2020

Informationsteknologi – Cybersikkerhed – Overblik og koncepter

Information technology – Cybersecurity – Overview and concepts

DANSK STANDARD
Danish Standards Association

Göteborg Plads 1
DK-2150 Nordhavn

Tel: +45 39 96 61 01

dansk.standard@ds.dk

www.ds.dk

DS projekt: M345886
ICS: 35.030

Første del af denne publikations betegnelse er:
DS/ISO/IEC TS, hvilket betyder, at det er en international teknisk specifikation, der har status som DS-information.

Denne publikations overensstemmelse er:
IDT med: ISO/IEC TS 27100:2020

DS-publikationen er på engelsk.

DS-publikationstyper

Dansk Standard udgiver forskellige publikationstyper.
Typen på denne publikation fremgår af forsiden.

Der kan være tale om:

Dansk standard

- standard, der er udarbejdet på nationalt niveau, eller som er baseret på et andet lands nationale standard, eller
- standard, der er udarbejdet på internationalt og/eller europæisk niveau, og som har fået status som dansk standard

DS-information

- publikation, der er udarbejdet på nationalt niveau, og som ikke har opnået status som standard, eller
- publikation, der er udarbejdet på internationalt og/eller europæisk niveau, og som ikke har fået status som standard, fx en teknisk rapport, eller
- europæisk præstandard

DS-håndbog

- samling af standarder, eventuelt suppleret med informativt materiale

DS-hæfte

- publikation med informativt materiale

Til disse publikationstyper kan endvidere udgives

- tillæg og rettelsesblade

DS-publikationsform

Publikationstyperne udgives i forskellig form som henholdsvis

• fuldtekstpublikation	(publikationen er trykt i sin helhed)
• godkendelsesblad	(publipukationen leveres i kopi med et trykt DS-omslag)
• elektronisk	(publikationen leveres på et elektronisk medie)

DS-betegnelse

Alle DS-publikationers betegnelse begynder med DS efterfulgt af et eller flere præfikser og et nr., fx **DS 383**, **DS/EN 5414** osv. Hvis der efter nr. er angivet et **A** eller **Cor**, betyder det, enten at det er et **tillæg** eller et **rettelsesblad** til hovedstandarden, eller at det er indført i hovedstandarden.
DS-betegnelse angives på forsiden.

Overensstemmelse med anden publikation:

Overensstemmelse kan enten være IDT, EQV, NEQ eller MOD

• **IDT:**	Når publikationen er identisk med en given publikation.
• **EQV:**	Når publikationen teknisk er i overensstemmelse med en given publikation, men præsentationen er ændret.
• **NEQ:**	Når publikationen teknisk eller præsentationsmæssigt ikke er i overensstemmelse med en given standard, men udarbejdet på baggrund af denne.
• **MOD:**	Når publikationen er modificeret i forhold til en given publikation.

DS/ISO/IEC TS 27100:2020

TECHNICAL

ISO/IEC TS

First edition
2020-12-22

Information technology — Cybersecurity — Overview and concepts

Informationsteknologi – Cybersikkerhed – Overblik og koncepter

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

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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*