Informationsteknologi – Sikkerhedsteknikker – Ledelsessystemer for informationssikkerhed – Oversigt og ordliste

Information technology – Security techniques – Information security management systems – Overview and vocabulary

DANSK STANDARD
Danish Standards Association

Göteborg Plads 1
DK-2150 Nordhavn

Tel: +45 39 96 61 01
Tel: +45 39 96 61 01
dansk.standard@ds.dk
www.ds.dk

DS projekt: M321452
ICS: 01.040.35; 03.100.70; 35.030

Første del af denne publikations betegnelse er:
DS/ISO/IEC, hvilket betyder, at det er en international standard, der har status som dansk standard.

Denne publikations overensstemmelse er:
IDT med: ISO/IEC 27000:2018

DS-publikationen er på dansk og engelsk.

Denne publikation erstatter: DS/ISO/IEC 27000:2016

I tilfælde af tvivl om oversættelsens korrekthed henvises til den engelske version.

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.

INTERNATIONAL ISO/IEC

Fifth edition
2018-02-01

Information technology — Security techniques — Information security management systems — Overview and vocabulary

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire

Reference number
ISO/IEC 27000:2018(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

Indholdsfortegnelse

Side

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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 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).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

This fifth edition cancels and replaces the fourth edition (ISO/IEC 27000:2016), which has been technically revised. The main changes compared to the previous edition are as follows:

— the Introduction has been reworded;

— some terms and definitions have been removed;

— Clause 3 has been aligned on the high-level structure for MSS;

— Clause 5 has been updated to reflect the changes in the standards concerned;

— Annexes A and B have been deleted.

Forord

ISO (International Organization for Standardization) er en verdensomspændende sammenslutning af nationale standardiseringsorganisationer (ISO's medlemsorganisationer). Internationale Standarder udarbejdes normalt af ISO's tekniske komiteer. Hver medlemsorganisation, som er interesseret i et emne, inden for hvilket der er oprettet en teknisk komite, har ret til at være repræsenteret i den pågældende komite. Internationale organisationer, både statslige og ikke-statslige, der har en samarbejdsaftale med ISO, deltager ligeledes i arbejdet. ISO samarbejder tæt med IEC (International Electrotechnical Commission) i alle forhold vedrørende elektroteknisk standardisering.

De procedurer, der er anvendt ved udarbejdelsen af dette dokument og de procedurer, der er beregnet til vedligeholdelse af dokumentet, er beskrevet i ISO/IEC Directives, Part 1. Især bør de forskellige godkendelseskriterier, der er nødvendige for de forskellige typer ISO-dokumenter, bemærkes. Dette dokument er udarbejdet i overensstemmelse med de redaktionelle regler opstillet i ISO/IEC Directives, Part 2 (se www.iso.org/directives).

Der gøres opmærksom på, at indhold i dette dokument kan være underlagt patentrettigheder. ISO kan ikke drages til ansvar for at identificere sådanne patentrettigheder. Detaljerede oplysninger om eventuelle patentrettigheder, der konstateres under udarbejdelsen af dette dokument, findes i Indledningen og/eller på ISO's liste over modtagne patenterklæringer (se www.iso.org/patents).

Eventuelle handelsnavne i dette dokument er givet af hensyn til brugerne og indebærer ikke en godkendelse.

En forklaring af standardernes frivillige natur, betydningen af ISO-specifikke termer og udtryk vedrørende overensstemmelseserklæring samt oplysninger om ISO's overholdelse af WTO-principperne vedrørende tekniske handelshindringer (TBT) findes på websitet: www.iso.org/iso/foreword.html.

Dette dokument er udarbejdet af teknisk komite ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

Denne 5. udgave ophæver og erstatter 4. udgave (ISO/IEC 27000:2016), hvis indhold er blevet teknisk revideret. De væsentligste ændringer i forhold til den tidligere udgave er følgende

— Indledningen er blevet omformuleret.

— Nogle termer og definitioner er blevet fjernet.

— Punkt 3 er blevet tilpasset den overordnede struktur for MSS

— Punkt 5 er blevet ajourført og afspejler nu ændringerne i de pågældende standarder.

— Anneks A og B er blevet slettet.

Introduction

0.1 Overview

International Standards for management systems provide a model to follow in setting up and operating a management system. This model incorporates the features on which experts in the field have reached a consensus as being the international state of the art. ISO/IEC JTC 1/SC 27 maintains an expert committee dedicated to the development of international management systems standards for information security, otherwise known as the Information Security Management system (ISMS) family of standards.

Through the use of the ISMS family of standards, organizations can develop and implement a framework for managing the security of their information assets, including financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties. These standards can also be used to prepare for an independent assessment of their ISMS applied to the protection of information.

0.2 Purpose of this document

The ISMS family of standards includes standards that:

a) define requirements for an ISMS and for those certifying such systems;

b) provide direct support, detailed guidance and/or interpretation for the overall process to establish, implement, maintain, and improve an ISMS;

c) address sector-specific guidelines for ISMS; and

d) address conformity assessment for ISMS.

0.3 Content of this document

In this document, the following verbal forms are used:

— “shall” indicates a requirement;

— “should” indicates a recommendation;

— “may” indicates a permission;

— “can” indicates a possibility or a capability.

Information marked as "NOTE" is for guidance in understanding or clarifying the associated requirement. “Notes to entry” used in Clause 3 provide additional information that supplements the terminological data and can contain provisions relating to the use of a term.

Indledning

0.1 Oversigt

Internationale standarder for ledelsessystemer opstiller en model, der kan følges ved oprettelse og drift af et ledelsessystem. Denne model omfatter de elementer, som eksperter inden for området er blevet enige om som værende det aktuelle internationale tekniske niveau.ISO/IEC JTC 1/SC 27 har et ekspertudvalg for udarbejdelse af internationale ledelsessystemstandarder for informationssikkerhed, også kendt som standarderne for ledelsessystemer for informationssikkerhed (ISMS).

Ved hjælp af ISMS-standarderne kan organisationer udvikle og implementere rammer for sikkerhedsledelse af deres informationsaktiver, herunder finansielle data, intellektuel ejendom og medarbejderoplysninger eller information, organisationerne har fået af kunder eller tredjeparter. Disse standarder kan også bruges til at udarbejde en uafhængig vurdering af organisationernes ISMS med henblik på beskyttelse af oplysninger.

0.2 Formålet med dette dokument

ISMS-standarderne omfatter standarder, som:

a) definerer krav til et ISMS og dem, der certificerer sådanne systemer

b) giver direkte støtte, detaljeret vejledning og/eller fortolkning i forbindelse med den overordnede proces til etablering, implementering, vedligeholdelse og forbedring af et ISMS

c) beskriver sektorspecifikke retningslinjer for ISMS og

d) beskriver overensstemmelsesvurdering for ISMS.

0.3 Indholdet i dette dokument

I dette dokument anvendes følgende verbalformer:

— “skal” udtrykker et krav

— “bør” udtrykker en anbefaling

— ”kan” udtrykker en tilladelse,

en mulighed eller en evne.

Tekst mærket med ”NOTE” er en vejledning til forståelse eller afklaring af det tilhørende krav. “Noter til term”, der er anvendt i pkt. 3, giver yderligere oplysninger, som supplerer de terminologiske data, og kan indeholde bestemmelser vedrørende brugen af en term.

1 Scope

This document provides the overview of information security management systems (ISMS). It also provides terms and definitions commonly used in the ISMS family of standards. This document is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations).

The terms and definitions provided in this document

— cover commonly used terms and definitions in the ISMS family of standards;

— do not cover all terms and definitions applied within the ISMS family of standards; and

— do not limit the ISMS family of standards in defining new terms for use.

2 Normative references

There are no normative references in this document.

Informationsteknologi – Sikkerhedsteknikker – Ledelsessystemer for informationssikkerhed – Oversigt og ordliste

1 Anvendelsesområde

Dette dokument indeholder en oversigt over ledelsessystemer for informationssikkerhed (ISMS). Det indeholder også de mest anvendte termer og definitioner i ISMS-standarderne. Dette dokument gælder for alle typer og størrelser af organisationer (fx kommercielle virksomheder, offentlige myndigheder, almennyttige organisationer).

De termer og definitioner, der er angivet i dette dokument

— dækker hyppigt anvendte termer og definitioner i ISMS-standarderne

— dækker ikke alle anvendte termer og definitioner i ISMS-standarderne og

— begrænser ikke ISMS-standarderne i definitionen af nye termer.

2 Normative referencer

Der er ingen normative referencer i dette dokument.