Informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse – Foranstaltninger til informationssikkerhed

Information security, cybersecurity and privacy protection – Information security controls (ISO/IEC 27002:2022)

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: M362244
ICS: 35.030

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

Denne publikations overensstemmelse er:
IDT med: ISO/IEC 27002:2022
IDT med: EN ISO/IEC 27002:2022

DS-publikationen er på dansk og engelsk.

Denne publikation erstatter: DS/EN ISO/IEC 27002:2017

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 (publikationen 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.

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

November 2022

ICS 35.030

English Version

Information security, cybersecurity and privacy protection - Information security controls (ISO/IEC 27002:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée - Moyens de maîtrise de l'information (ISO/IEC 27002:2022)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022)

This European Standard was approved by CEN on 30 October 2022.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Europæisk forord (EN)

Teksten til ISO/IEC 27002:2022 er udarbejdet af teknisk komite ISO/IEC JTC 1 "Information technology" under den internationale standardiseringsorganisation ISO og er godkendt som EN ISO/IEC 27002:2022 af teknisk komite CEN-CENELEC/JTC 13 "Cybersecurity and Data Protection", hvis sekretariat varetages af DIN.

Denne Europæiske Standard skal inden maj 2023 have status som national standard enten ved udgivelse af en identisk tekst eller ved formel godkendelse, og modstridende nationale standarder skal være trukket tilbage senest maj 2023.

Der gøres opmærksom på, at indhold i dette dokument kan være underlagt patentrettigheder. CEN-CENELEC kan ikke drages til ansvar for at identificere sådanne patentrettigheder.

Dette dokument erstatter EN ISO/IEC 27002:2017.

Tilbagemeldinger og spørgsmål vedrørende dette dokument bør rettes til brugerens nationale standardiseringsorganisation. En fuldstændig liste over disse organisationer findes på CEN og CENELEC's hjemmeside.

I henhold til CEN/CENELEC's Internal Regulations er de nationale standardiseringsorganisationer i følgende lande forpligtet til at implementere denne Europæiske Standard: Belgien, Bulgarien, Cypern, Danmark, Estland, Finland, Frankrig, Grækenland, Irland, Island, Italien, Kroatien, Letland, Litauen, Luxembourg, Malta, Nederlandene, Norge, Polen, Portugal, Republikken Nordmakedonien, Rumænien, Schweiz, Serbien, Slovakiet, Slovenien, Spanien, Storbritannien, Sverige, Tjekkiet, Tyrkiet, Tyskland, Ungarn og Østrig.

Godkendelse

Teksten i ISO/IEC 27002:2022 er godkendt af CEN-CENELEC som EN ISO/IEC 27002:2022 uden ændringer.

INTERNATIONAL ISO/IEC

Third edition
2022-02

Corrected version
2022-02-15

Information security, cybersecurity and privacy protection — Information security controls

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information

Reference number
ISO/IEC 27002:2022(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

Indholdsfortegnelse (EN)

Side

Forord (EN)

ISO (International Organization for Standardization) og IEC (International Electrotechnical Commission) er de to verdensomspændende organisationer for standardisering. Nationale medlemsorganisationer af ISO eller IEC deltager i udarbejdelsen af Internationale Standarder i tekniske komiteer, som ISO eller IEC har nedsat på særlige tekniske områder. Tekniske komiteer under ISO og IEC samarbejder inden for områder af fælles interesse. Andre internationale organisationer, både statslige og ikke-statslige, der har en samarbejdsaftale med ISO og IEC, deltager ligeledes i arbejdet.

De procedurer, der er anvendt ved udarbejdelsen af dette dokument og dem, 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 dokumenter, bemærkes. Dette dokument er udarbejdet i overensstemmelse med de redaktionelle regler i ISO/IEC Directives, Part 2 (se www.iso.org/directives eller www.iec.ch/members_experts/refdocs).

Der gøres opmærksom på, at indhold i dette dokument kan være underlagt patentrettigheder. ISO og IEC 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) eller IEC's liste over modtagne patenterklæringer (se patents.iec.ch).

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

Websitet www.iso.org/iso/foreword.html giver en redegørelse for standardernes karakter af frivillighed, betydningen af ISO-specifikke termer og udtryk vedrørende overensstemmelseserklæring samt oplysninger om ISO's overholdelse af WTO-principperne for tekniske handelshindringer (TBT). For IEC se www.iec.ch/understanding-standards.

Dette dokument er udarbejdet af den fælles tekniske komite ISO/IEC JTC 1, *Information technology*, underkomite SC 27, *Information security, cybersecurity and privacy protection*.

Denne 3. udgave ophæver og erstatter 2. udgave (ISO/IEC 27002:2013), hvis indhold er blevet teknisk revideret. Rettelsesbladet ISO/IEC 27002:2013/Cor. 1:2014 og ISO/IEC 27002:2013/Cor. 2:2015. er også indarbejdet.

De væsentligste ændringer er følgende:

- titlen er ændret
- dokumentets struktur er ændret og præsenterer nu foranstaltningerne ved hjælp af en simpel taksonomi og tilhørende attributter
- nogle foranstaltninger er blevet lagt sammen, nogle er blevet slettet, og en række nye foranstaltninger er blevet indført. Se anneks B for et samlet overblik over sammenhængen.

Denne rettede udgave af ISO/IEC 27002:2022 indeholder følgende rettelser:

— ikke-fungerende hyperlinks i hele dokumentet er gendannet

— i den indledende tabel i 5.22 og i tabel A.1 (række 5.22) er "#Sikring_af_informationssikkerhed" flyttet fra kolonnen "Sikkerhedsdomæner" til kolonnen "Driftsmæssige kapaciteter".

Tilbagemeldinger eller spørgsmål vedrørende dette dokument bør rettes til brugerens nationale standardiseringsorganisation. En fuldstændig liste over disse organisationer findes på www.iso.org/members.html og www.iec.ch/national-committees.

Indledning (EN)

0.1 Baggrund og sammenhæng

Dette dokument er udarbejdet til organisationer af alle typer og størrelser. Det er hensigten, at det anvendes som en reference til at fastlægge og implementere foranstaltninger til håndtering af informationssikkerhedsrisici i et ledelsessystem for informationssikkerhed (ISMS), der er baseret på ISO/IEC 27001. Det kan også anvendes som et vejledende dokument for organisationer, der vil fastlægge og implementere almindeligt accepterede informationssikkerhedsforanstaltninger. Dette dokument er derudover beregnet til brug ved udarbejdelsen af branche- og organisationsspecifikke retningslinjer for informationssikkerhedsledelse under hensyntagen til det/de specifikke informationssikkerhedsmæssige risikomiljø(er). Andre organisatoriske eller miljøspecifikke foranstaltninger end dem, der er indeholdt i dette dokument, kan fastlægges ved hjælp af en risikovurdering, hvor det er nødvendigt.

Organisationer af alle typer og størrelser (herunder offentlige, private, kommercielle og almennyttige) udarbejder, indsamler, behandler, lagrer, transmitterer og bortskaffer mange former for information, herunder elektronisk, fysisk og verbal information (fx samtaler og præsentationer).

Værdien af information strækker sig ud over skrevne ord, tal og billeder: viden, begreber, ideer og varemærker er eksempler på immateriel information. I en verden med stor sammenhængskraft fortjener eller kræver information og understøttende aktiver beskyttelse mod forskellige risikokilder, uanset om disse er naturlige, tilfældige eller tilsigtede.

Informationssikkerhed opnås ved at implementere et passende sæt foranstaltninger, herunder politikker, regler, processer, procedurer, organisationsstrukturer samt software- og hardwarefunktioner. For at kunne opfylde specifikke sikkerheds- og forretningsmæssige mål bør organisationen definere, implementere, overvåge, vurdere og forbedre disse foranstaltninger, hvor det er nødvendigt. Der anlægges i et ISMS som det, der er beskrevet i ISO/IEC 27001, en holistisk koordineret fremstilling af organisationens informationssikkerhedsrisici med henblik på at fastlægge og implementere en omfattende række af informationssikkerhedsforanstaltninger inden for de overordnede rammer af et sammenhængende ledelsessystem.

Mange informationssystemer, herunder styring og drift af disse systemer, har ikke et forsvarligt sikkerhedsniveau i form af et ISMS i henhold til ISO/IEC 27001 og dette dokument. Det sikkerhedsniveau, der kan opnås udelukkende ved hjælp af teknologiske midler, er begrænset og bør understøttes af passende ledelsesaktiviteter og organisatoriske processer. Det kræver omhyggelig planlægning og detaljefokus at identificere, hvilke foranstaltninger der bør iværksættes, samtidig med at der iværksættes risikohåndtering.

Det kræver medvirken fra alle medarbejderne i organisationen at opbygge et vellykket ISMS. Der kan også være behov for deltagelse af andre interessenter, såsom aktionærer og leverandører. Derudover kan der være behov for ekstern ekspertbistand.

Et egnet, fyldestgørende og effektivt ISMS giver organisationens ledelse og andre interessenter sikkerhed for, at information og understøttende aktiver er forholdsvis sikre og beskyttet mod trusler og skadevirkninger og dermed gør det muligt for organisationen at nå de erklærede forretningsmål.

0.2 Informationssikkerhedskrav

Det er vigtigt, at en organisation fastlægger sine informationssikkerhedskrav. Der er tre hovedkilder af informationssikkerhedskrav:

a) Vurdering af risici i organisationen, idet der tages højde for organisationens overordnede forretningsstrategi og målsætninger. Den kan faciliteres eller understøttes gennem en informationssikkerhedsspecifik risikovurdering. Vurderingen bør resultere i en fastlæggelse af, hvilke foranstaltninger der er nødvendige for at sikre, at organisationens restrisiko opfylder kriterierne for risikovillighed.

b) juridiske, lovmæssige, regulatoriske og kontraktlige krav, som en organisation og dens interessenter (handelspartnere, og serviceudbydere m.fl.) skal opfylde, samt hensynet til det sociokulturelle miljø.

c) Sæt af principper, målsætninger og forretningsmæssige krav til alle trin i den livscyklus for information, som en organisation har udviklet for at understøtte driften.

0.3 Foranstaltninger

En foranstaltning defineres som et tiltag, der ændrer eller bevarer en risiko. Nogle foranstaltninger i dette dokument ændrer risici, mens andre bevarer risici. En informationssikkerhedspolitik kan fx kun bevare risici, hvorimod overholdelse af informationssikkerhedspolitikken kan ændre risici. Desuden beskriver nogle foranstaltninger samme generiske tiltag i forskellige risikosammenhænge. Dette dokument indeholder en generisk blanding af organisatoriske, personrelaterede, fysiske og teknologiske informationssikkerhedsforanstaltninger, der er afledt af internationalt anerkendt best practice.

0.4 Fastlæggelse af foranstaltninger

Fastlæggelse af foranstaltninger afhænger af organisationens beslutninger efter en risikovurdering med et klart defineret omfang. Beslutninger vedrørende identificerede risici bør baseres på kriterierne for risikovillighed, risikohåndteringsmuligheder og den risikostyringsmetode, som organisationen anvender. Når der fastlægges foranstaltninger, bør det ske i henhold til alle relevante nationale og internationale love og forskrifter. Fastlæggelse af foranstaltninger afhænger også af den måde, hvorpå foranstaltningerne påvirker hinanden og på den måde udgør et forsvar i dybden.

Organisationen kan skræddersy foranstaltninger efter behov eller identificere dem fra anden kilde. Ved specificering af sådanne foranstaltninger bør organisationen overveje, hvilke ressourcer og investeringer der er nødvendige for at implementere og drive en foranstaltning i forhold til den forretningsmæssige værdi, der realiseres. Se ISO/IEC TR 27016 for vejledning om beslutninger vedrørende investeringen i et ISMS og de økonomiske konsekvenser ved disse beslutninger i forbindelse med konkurrerende krav til ressourcer.

Der bør være balance mellem de anvendte ressourcer til implementering af foranstaltninger og den potentielle konsekvens af sikkerhedsincidents, hvis disse foranstaltninger ikke findes. Resultaterne af en risikovurdering bør være en hjælp til at vise vej til og fastlægge relevante ledelsestiltag, prioriteringer til at styre informationssikkerhedsrisici samt implementere foranstaltninger, der er vurderet som værende nødvendige for at beskytte mod disse risici.

Nogle af foranstaltningerne i dette dokument kan betragtes som vejledende principper for informationssikkerhedsledelse og som værende anvendelige for de fleste organisationer. For yderligere information om fastlæggelse af foranstaltninger og andre risikohåndteringsmuligheder, se ISO/IEC 27005.

0.5 Udarbejdelse af organisationsspecifikke retningslinjer

Dette dokument kan betragtes som et udgangspunkt for udarbejdelse af organisationsspecifikke retningslinjer. Ikke alle foranstaltninger og vejledninger i dette dokument er relevante for alle organisationer. Foranstaltninger og retningslinjer, der ikke er indeholdt i dette dokument, kan også være nødvendige for at adressere organisationens specifikke behov og de identificerede risici. Når der udarbejdes dokumenter med andre retningslinjer eller foranstaltninger, kan det være nyttigt at medtage krydshenvisninger til punkter i dette dokument til senere brug.

0.6 Overvejelser om livscyklus

Information har en livscyklus fra udarbejdelse til bortskaffelse. Værdien af information og forbundne risici kan variere i løbet af levetiden (fx har uautoriseret videregivelse eller tyveri af et selskabs regnskab ingen betydning, efter regnskabet er offentliggjort, men integriteten er stadig kritisk), og informationssikkerhed forbliver derfor centralt i et vist omfang på alle niveauer.

Informationssystemer og andre aktiver, der er relevante for informationssikkerhed, har livscyklusser, inden for hvilke de udtænkes, specificeres, udformes, udarbejdes, testes, implementeres, anvendes,

vedligeholdes og til slut tages ud af drift og bortskaffes. Der bør tages højde for informationssikkerhed i alle faser. Nye systemudviklingsprojekter og ændringer af eksisterende systemer giver muligheder for at forbedre sikkerhedsforanstaltningerne under hensyntagen til organisationens risici og erfaringer fra incidents.

0.7 Relaterede internationale standarder

Hvor dette dokument giver vejledning om en bred vifte af informationssikkerhedsforanstaltninger, som anvendes i mange forskellige organisationer, indeholder andre dokumenter i ISO/IEC 27000-serien supplerende råd eller krav vedrørende andre aspekter i den overordnede proces for håndtering af informationssikkerhed.

Der henvises til ISO/IEC 27000 for en generel introduktion til både ISMS og ISMS-dokumenterne. ISO/IEC 27000 indeholder en ordliste, som definerer de fleste af de termer, som anvendes i ISO/IEC 27000-serien, og beskriver anvendelsesområde og målsætninger for hvert dokument i serien.

Sektorspecifikke standarder med supplerende foranstaltninger har til formål at dække specifikke områder (fx ISO/IEC 27017 for cloudtjenester, ISO/IEC 27701 for privatlivsbeskyttelse, ISO/IEC 27019 for energi, ISO/IEC 27011 for telekommunikationsorganisationer og ISO 27799 for sundhed). Disse standarder er indeholdt i bibliografien, og nogle af dem er henvist til i vejledningen og andre informationsafsnit i pkt. 5-8.

Informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse – Foranstaltninger til informationssikkerhed

1 Anvendelsesområde (EN)

Dette dokument indeholder et referencesæt af generiske informationssikkerhedsforanstaltninger, inklusiv implementeringsvejledning. Dette dokument er udarbejdet til brug for organisationer

a) inden for rammerne af et ledelsessystem for informationssikkerhed (ISMS), der er baseret på ISO/IEC 27001

b) til implementering af informationssikkerhedsforanstaltninger, der er baseret på internationalt anerkendt best practice

c) til udvikling af organisationsspecifikke retningslinjer for informationssikkerhedsledelse.

2 Normative referencer (EN)

Der er ingen normative referencer i dette dokument.

European foreword (DA)

The text of ISO/IEC 27002:2022 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 27002:2022 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by May 2023, and conflicting national standards shall be withdrawn at the latest by May 2023.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO/IEC 27002:2017.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/IEC 27002:2022 has been approved by CEN-CENELEC as EN ISO/IEC 27002:2022 without any modification.

Contents (DA)

Page

Foreword (DA)

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 or www.iec.ch/members_experts/refdocs).

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. In the IEC, see www.iec.ch/understanding-standards.

'This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 27002:2013), which has been technically revised. It also incorporates the Technical Corrigenda ISO/IEC 27002:2013/Cor. 1:2014 and ISO/IEC 27002:2013/Cor. 2:2015.

The main changes are as follows:

— the title has been modified;

— the structure of the document has been changed, presenting the controls using a simple taxonomy and associated attributes;

— some controls have been merged, some deleted and several new controls have been introduced. The complete correspondence can be found in Annex B.

This corrected version of ISO/IEC 27002:2022 incorporates the following corrections:

— non-functioning hyperlinks throughout the document have been restored;

— in the introductory table in subclause 5.22 and in Table A.1 (row 5.22), "#information_security_assurance" has been moved from the column headed "Security domains" to the column headed "Operational capabilities".

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 and www.iec.ch/national-committees.

Introduction (DA)

0.1 Background and context

This document is designed for organizations of all types and sizes. It is to be used as a reference for determining and implementing controls for information security risk treatment in an information security management system (ISMS) based on ISO/IEC 27001. It can also be used as a guidance document for organizations determining and implementing commonly accepted information security controls. Furthermore, this document is intended for use in developing industry and organization-specific information security management guidelines, taking into consideration their specific information security risk environment(s). Organizational or environment-specific controls other than those included in this document can be determined through risk assessment as necessary.

Organizations of all types and sizes (including public and private sector, commercial and non-profit) create, collect, process, store, transmit and dispose of information in many forms, including electronic, physical and verbal (e.g. conversations and presentations).

The value of information goes beyond written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information. In an interconnected world, information and other associated assets deserve or require protection against various risk sources, whether natural, accidental or deliberate.

Information security is achieved by implementing a suitable set of controls, including policies, rules, processes, procedures, organizational structures and software and hardware functions. To meet its specific security and business objectives, the organization should define, implement, monitor, review and improve these controls where necessary. An ISMS such as that specified in ISO/IEC 27001 takes a holistic, coordinated view of the organization's information security risks in order to determine and implement a comprehensive suite of information security controls within the overall framework of a coherent management system.

Many information systems, including their management and operations, have not been designed to be secure in terms of an ISMS as specified in ISO/IEC 27001 and this document. The level of security that can be achieved only through technological measures is limited and should be supported by appropriate management activities and organizational processes. Identifying which controls should be in place requires careful planning and attention to detail while carrying out risk treatment.

A successful ISMS requires support from all personnel in the organization. It can also require participation from other interested parties, such as shareholders or suppliers. Advice from subject matter experts can also be needed.

A suitable, adequate and effective information security management system provides assurance to the organization's management and other interested parties that their information and other associated assets are kept reasonably secure and protected against threats and harm, thereby enabling the organization to achieve the stated business objectives.

0.2 Information security requirements

It is essential that an organization determines its information security requirements. There are three main sources of information security requirements:

a) the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. This can be facilitated or supported through an information security-specific risk assessment. This should result in the determination of the controls necessary to ensure that the residual risk to the organization meets its risk acceptance criteria;

b) the legal, statutory, regulatory and contractual requirements that an organization and its interested parties (trading partners, service providers, etc.) have to comply with and their socio-cultural environment;

c) the set of principles, objectives and business requirements for all the steps of the life cycle of information that an organization has developed to support its operations.

0.3 Controls

A control is defined as a measure that modifies or maintains risk. Some of the controls in this document are controls that modify risk, while others maintain risk. An information security policy, for example, can only maintain risk, whereas compliance with the information security policy can modify risk. Moreover, some controls describe the same generic measure in different risk contexts. This document provides a generic mixture of organizational, people, physical and technological information security controls derived from internationally recognized best practices.

0.4 Determining controls

Determining controls is dependent on the organization's decisions following a risk assessment, with a clearly defined scope. Decisions related to identified risks should be based on the criteria for risk acceptance, risk treatment options and the risk management approach applied by the organization. The determination of controls should also take into consideration all relevant national and international legislation and regulations. Control determination also depends on the manner in which controls interact with one another to provide defence in depth.

The organization can design controls as required or identify them from any source. In specifying such controls, the organization should consider the resources and investment needed to implement and operate a control against the business value realized. See ISO/IEC TR 27016 for guidance on decisions regarding the investment in an ISMS and the economic consequences of these decisions in the context of competing requirements for resources.

There should be a balance between the resources deployed for implementing controls and the potential resulting business impact from security incidents in the absence of those controls. The results of a risk assessment should help guide and determine the appropriate management action, priorities for managing information security risks and for implementing controls determined necessary to protect against these risks.

Some of the controls in this document can be considered as guiding principles for information security management and as being applicable for most organizations. More information about determining controls and other risk treatment options can be found in ISO/IEC 27005.

0.5 Developing organization-specific guidelines

This document can be regarded as a starting point for developing organization-specific guidelines. Not all of the controls and guidance in this document can be applicable to all organizations. Additional controls and guidelines not included in this document can also be required to address the specific needs of the organization and the risks that have been identified. When documents are developed containing additional guidelines or controls, it can be useful to include cross-references to clauses in this document for future reference.

0.6 Life cycle considerations

Information has a life cycle, from creation to disposal. The value of, and risks to, information can vary throughout this life cycle (e.g. unauthorized disclosure or theft of a company's financial accounts is not significant after they have been published, but integrity remains critical) therefore, information security remains important to some extent at all stages.

Information systems and other assets relevant to information security have life cycles within which they are conceived, specified, designed, developed, tested, implemented, used, maintained and eventually retired from service and disposed of. Information security should be considered at every stage. New system development projects and changes to existing systems provide opportunities to improve security controls while taking into account the organization's risks and lessons learned from incidents.

0.7 Related International Standards

While this document offers guidance on a broad range of information security controls that are commonly applied in many different organizations, other documents in the ISO/IEC 27000 family provide complementary advice or requirements on other aspects of the overall process of managing information security.

Refer to ISO/IEC 27000 for a general introduction to both ISMS and the family of documents. ISO/IEC 27000 provides a glossary, defining most of the terms used throughout the ISO/IEC 27000 family of documents, and describes the scope and objectives for each member of the family.

There are sector-specific standards that have additional controls which aim at addressing specific areas (e.g. ISO/IEC 27017 for cloud services, ISO/IEC 27701 for privacy, ISO/IEC 27019 for energy, ISO/IEC 27011 for telecommunications organizations and ISO 27799 for health). Such standards are included in the Bibliography and some of them are referenced in the guidance and other information sections in Clauses 5-8.

Information security, cybersecurity and privacy protection — Information security controls

1 Scope (DA)

This document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:

a) within the context of an information security management system (ISMS) based on ISO/IEC 27001;

b) for implementing information security controls based on internationally recognized best practices;

c) for developing organization-specific information security management guidelines.

2 Normative references (DA)

There are no normative references in this document.