SVENSK STANDARD
SS-ISO/IEC 27000:2018

Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Översikt och terminologi (ISO/IEC 27000:2018)

Information technology – Security techniques – Information security management systems – Overview and vocabulary (ISO/IEC 27000:2018)

Svenska Institutet för Standarder

Språk: svenska/Swedish, engelska/English

Utgåva: 4

Svenska Institutet för Standarder

Den här standarden kan hjälpa dig att effektivisera och kvalitetssäkra ditt arbete. SIS har fler tjänster att erbjuda dig för att underlätta tillämpningen av standarder i din verksamhet.

SIS Abonnemang
Snabb och enkel åtkomst till gällande standard med SIS Abonnemang, en prenumerationstjänst genom vilken din organisation får tillgång till all världens standarder, senaste uppdateringarna och där hela din organisation kan ta del av innehållet i prenumerationen.

Utbildning, event och publikationer
Vi erbjuder även utbildningar, rådgivning och event kring våra mest sålda standarder och frågor kopplade till utveckling av standarder. Vi ger också ut handböcker som underlättar ditt arbete med att använda en specifik standard.

Vill du delta i ett standardiseringsprojekt?
Genom att delta som expert i någon av SIS 300 tekniska kommittéer inom CEN (europeisk standardisering) och/eller ISO (internationell standardisering) har du möjlighet att påverka standardiseringsarbetet i frågor som är viktiga för din organisation. Välkommen att kontakta SIS för att få veta mer!

Kontakt
Skriv till kundservice@sis.se, besök sis.se eller ring 08 - 555 523 10

Upplysningar om sakinnehållet i standarden lämnas av Svenska institutet för standarder, telefon 08 - 555 520 00. Standarder kan beställas hos SIS som även lämnar allmänna upplysningar om svensk och utländsk standard.

Standarden är framtagen av kommittén Informationssäkerhet, SIS/TK 318.

Har du synpunkter på innehållet i den här standarden, vill du delta i ett kommande revideringsarbete eller vara med och ta fram andra standarder inom området? Gå in på www.sis.se - där hittar du mer information.

Fastställd: 2018-11-09
ICS: 01.040.35; 04.050; 35.020; 35.040

Svenska Institutet för Standarder

Den internationella standarden SS-ISO/IEC 27000:2018 gäller som svensk standard. Detta dokument innehåller den svenska språkversionen av ISO/IEC 27000:2018 följd av den officiella engelska språkversionen.

Denna standard ersätter SS-ISO/IEC 27000:2016, utgåva 3.

The International Standard SS-ISO/IEC 27000:2018 has the status of a Swedish Standard. This document contains the Swedish language version of ISO/IEC 27000:2018 followed by the official English version.

This standard supersedes the Swedish Standard SS-ISO/IEC 27000:2016, edition 3.

Innehåll

Sida

Orientering ..... **v**

1 Omfattning **1**

2 Normativa referenser **1**

3 Termer och definitioner **1**

4 Ledningssystem för informationssäkerhet **12**
4.1 Allmänt 12
4.2 Vad är LIS? 12
4.2.1 Översikt och principer 12
4.2.2 Information 13
4.2.3 Informationssäkerhet 13
4.2.4 Förvaltning av ledningssystem 13
4.2.5 Ledningssystem 13
4.3 Processorientering 14
4.4 Varför LIS är viktigt 14
4.5 Upprätta, övervaka, underhålla och förbättra LIS 15
4.5.1 Översikt 15
4.5.2 Fastställande av krav på informationssäkerhet 15
4.5.3 Riskbedömning inom informationssäkerhet 15
4.5.4 Riskbehandling inom informationssäkerhet 16
4.5.5 Välja och vidta säkerhetsåtgärder 16
4.5.6 Övervaka, underhålla och förbättra effektiviteten i LIS 17
4.5.7 Ständig förbättring 17
4.6 Avgörande framgångsfaktorer i LIS 18
4.7 Nyttoeffekter med användningen av LIS-standarder 18

5 LIS-standarder **19**
5.1 Allmän information 19
5.2 Standarder som beskriver översikt och terminologi: SS-ISO/IEC 27000 (detta dokument) 19
5.3 Kravstandarder 20
5.3.1 ISO/IEC 27001 20
5.3.2 ISO/IEC 27006 20
5.3.3 ISO/IEC 27009 20
5.4 Vägledningsstandarder 21
5.4.1 ISO/IEC 27002 21
5.4.2 ISO/IEC 27003 21
5.4.3 ISO/IEC 27004 21
5.4.4 ISO/IEC 27005 21
5.4.5 ISO/IEC 27007 22
5.4.6 ISO/IEC TR 27008 22
5.4.7 ISO/IEC 27013 22
5.4.8 ISO/IEC 27014 23
5.4.9 ISO/IEC TR 27016 23
5.4.10 ISO/IEC 27021 23
5.5 Standarder som beskriver branschspecifika riktlinjer 24
5.5.1 ISO/IEC 27010 24
5.5.2 ISO/IEC 27011 24
5.5.3 ISO/IEC 27017 24
5.5.4 ISO/IEC 27018 25
5.5.5 ISO/IEC TR 27019 25
5.5.6 ISO 27799 26

Litteraturförteckning **27**

Förord

ISO (Internationella Standardiseringsorganisationen) är en världsomspännande sammanslutning av nationella standardiseringsorgan (ISO-medlemmar). Utarbetandet av internationella standarder sker normalt i ISOs tekniska kommittéer. Varje medlemsland som är intresserat av arbetet i en teknisk kommitté har rätt att bli medlem i den. Internationella organisationer, statliga såväl som icke-statliga, som samarbetar med ISO deltar också i arbetet. ISO har nära samarbete med International Electrotechnical Commission (IEC) i alla frågor rörande elektroteknisk standardisering.

Internationella standarder utarbetas i enlighet med ISO/IEC Directives, Part 2.

Huvuduppgiften för de tekniska kommittéerna är att utarbeta internationella standarder. Förslag till internationella standarder som godkänts av de tekniska kommittéerna sänds till medlemsländerna för röstning. För publicering av en internationell standard krävs att minst 75 % av de röstande medlemsländerna godkänner förslaget.

Det bör uppmärksammas att vissa beståndsdelar i denna internationella standard möjligen kan vara föremål för patenträtter. ISO ska inte hållas ansvarig för att identifiera någon eller alla sådana patenträtter.

Den internationella standarden ISO/IEC 27000:2018 har utarbetats av ISO/IEC JTC 1 "Information technology", underkommitté SC 27 "IT Security Techniques", inom International Organization for Standardization (ISO) och inom International Electrotechnical Commission (IEC).

Orientering

0.1 Allmänt

Internationella ledningssystemsstandarder erbjuder en modell för att inrätta och driva ett ledningssystem. Innehållet i denna modell har uppnåtts genom samförstånd mellan internationella experter inom området. ISO/IEC JTC 1/SC 27 upprätthåller en expertkommitté som ägnar sig åt utvecklingen av internationella ledningssystemstandarder för informationssäkerhet, även känd som standardserien LIS.

Genom standardserien LIS kan organisationer utveckla och införa ett ramverk för att hantera säkerheten för sina informationstillgångar, även ekonomisk information, immateriella rättigheter, och anställdas personuppgifter eller information som anförtrotts dem av kunder eller tredje part. Dessa standarder kan också användas i syfte att förbereda sig för en oberoende bedömning om hur organisationens LIS tillämpas för att skydda informationstillgångarna.

0.2 Syftet med detta dokument

Standardserien LIS omfattar standarder som:

a) specificerar kraven för ett LIS och för de som certifierar sådana system

b) ger direkt stöd, detaljerade anvisningar och/eller tolkning till den övergripande processen i syfte att upprätta, genomföra, underhålla och förbättra ett LIS

c) anger branschspecifika riktlinjer för LIS

d) anger hur bedömning av överensstämmelse med LIS kan utföras.

0.3 Innehållet i detta dokument

I det här dokumentet används följande verb med betydelse:

- ”ska” anger ett krav.
- ”bör” anger en rekommendation.
- ”får” anger tillåtelse.
- ”kan” anger en möjlighet eller förmåga.

Information som är markerad med ”ANM.” ger vägledning för att skapa förståelse för och tydliggöra det aktuella kravet. ”Anm. till termpost”, som används i avsnitt 3, ger ytterligare information som kompletterar den terminologiska informationen och kan innehålla riktlinjer relaterade till användningen av termen.

1 Omfattning

Detta dokument ger en översikt över ledningssystem för informationssäkerhet (LIS). Den innehåller också termer och definitioner som vanligen används i standardserien LIS. Detta dokument är tillämpligt på organisationer av alla typer och storlekar (t.ex. kommersiella företag, myndigheter, icke-vinstdrivande organisationer).

De termer och definitioner som återfinns i detta dokument

– inbegriper vanligt förekommande termer och definitioner i standardserien LIS

– utgörs inte av samtliga termer och definitioner som förekommer inom standardserien LIS

– begränsar inte möjligheten att definiera nya begrepp och skapa nya termer inom standardserien LIS.

2 Normativa referenser

Det finns inga normativa referenser i detta dokument.

3 Termer och definitioner

ISO och IEC tillhandahåller följande termdatabaser för användning i standardisering:

- ISO Online browsing platform: https://www.iso.org/obp
- IEC Electropedia: https://www.electropedia.org/

3.1
åtkomstkontroll
sätt att säkerställa att åtkomst till tillgångar auktoriseras eller begränsas utifrån *krav* (3.56) på verksamhet och säkerhet

Svensk ANM. I Terminologi för informationssäkerhet (SIS-TR 50) definieras ”åtkomstkontroll” som ’funktioner i ett system som syftar till att reglera och kontrollera en användares åtkomst till information och resurser’.

3.2
attack
försök att förstöra, exponera, förändra, inaktivera, stjäla eller skaffa sig obehörig åtkomst till en tillgång eller använda den på ett obehörigt sätt

Svensk ANM. I Terminologi för informationssäkerhet (SIS-TR 50) definieras ”attack” som ’enskild aktivitet som syftar till att åstadkomma skada eller störningar för en verksamhet’.

3.3
revision
systematisk, oberoende och dokumenterad *process* (3.54) som syftar till att skaffa revisionsbelägg och utvärdera dessa objektivt för att avgöra i vilken utsträckning revisionskriterierna har uppfyllts

Anm. 1 till termpost: En revision kan vara intern (förstapartsrevision) eller extern (andraparts- eller tredjepartsrevision), och den kan också vara en kombinerad revision, då två eller fler ämnesområden kombineras.

Anm. 2 till termpost: En intern revision utförs av organisationen själv, eller av en extern part på uppdrag av organisationen.

Anm. 3 till termpost: ”Revisionsbelägg” och ”revisionskriterier” definieras i ISO 19011.

3.4
revisionsomfattning
omfattning och avgränsningar av en *revision* (3.3)

[KÄLLA: ISO 19011:2011, 3.14, modifierad – Anm. 1 till termpost har tagits bort.]

3.5
autentisering
försäkran om att en påstådd egenskap hos ett objekt är korrekt

Svensk ANM. I Terminologi för informationssäkerhet (SIS-TR 50) definieras ”autentisering” som ’verifiering av ett påstående’.

3.6
autenticitet
egenskapen att ett objekt är vad det utger sig för att vara

Svensk ANM. I Terminologi för informationssäkerhet (SIS-TR 50) definieras ”autenticitet” som ’äkthet avseende uppgivna uppgifter; särskilt rörande påstådd identitet och meddelandens ursprung och innehåll’.

3.7
tillgänglighet
egenskapen att vara åtkomlig och användbar på begäran från ett behörigt objekt

Svensk ANM. I Terminologi för informationssäkerhet (SIS-TR 50) definieras ”tillgänglighet” som ’åtkomst för behörig person vid rätt tillfälle’.

3.8
basmått
mått (3.42) definierat **i** form av ett attribut samt metoden för att kvantifiera detta attribut

[ISO/IEC 15939]

Anm. till termpost: Ett basmått är funktionellt oberoende av andra *mått.*

[KÄLLA: ISO/IEC 15939:2007, 2.3, modifierad – Anm. 2 till termpost har tagits bort.]

3.9
kompetens
förmåga att tillämpa kunskap och färdigheter för att uppnå avsedda resultat

3.10
konfidentialitet
egenskap som innebär att information inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller *processer* (3.54)

Svensk ANM. I Terminologi för informationssäkerhet (SIS-TR 50) definieras ”konfidentialitet” som ’skydd mot obehörig insyn’.

3.11
överensstämmelse
uppfyllande av ett *krav* (3.56)

3.12
konsekvens
resultat av en *händelse* (3.21) som påverkar *mål* (3.49)

Anm. 1 till termpost: En händelse kan få flera konsekvenser.

Anm. 2 till termpost: Konsekvenser kan vara såväl säkra som ovissa och är inom informationssäkerhetsområdet vanligtvis negativa.

ANM. 3: Konsekvenser kan uttryckas både kvalitativt och kvantitativt.

ANM. 4: Initiala konsekvenser kan trappas upp genom dominoeffekter.

[KÄLLA: ISO Guide 73:2009, 3.6.1.3, modifierad]

3.13
ständig förbättring
återkommande aktivitet för att förbättra *prestanda* (3.52)

3.14
säkerhetsåtgärd
åtgärd som förändrar en *risk* (3.61)

Anm. 1 till termpost: Säkerhetsåtgärder inkluderar varje *process* (3.54), *policy* (3.53), utrustning, praxis eller annan åtgärd som förändrar en *risk* (3.61).

Anm. 2 till termpost: Säkerhetsåtgärder får inte alltid avsedd eller förväntad effekt.

Svensk ANM. 1 I Terminologi för informationssäkerhet (SIS-TR 50) definieras ”säkerhetsåtgärd” som ’identifierad uppsättning åtgärder för att möta en organisations risker’.

Svensk ANM. 2 Säkerhetsåtgärder för informationssäkerhet omfattar åtgärder inom det administrativa och tekniska säkerhetsområdet.

Svensk ANM. 3 Säkerhetsåtgärder kan kategoriseras utifrån den tidpunkt då säkerhetsincidenten inträffade.

Svensk ANM. 4 I ISO 31000:2018 översätts ”control” till ”riskhanteringsåtgärd” och definitionen för begreppet översätts till ’åtgärd för att bibehålla och/eller förändra risker’.

3.15
säkerhetsmål
beskrivning av vad som ska uppnås som ett resultat av införd *säkerhetsåtgärd* (3.14)

3.16
korrigering
aktivitet för att eliminera en upptäckt *avvikelse* (3.47)

3.17
korrigerande åtgärd
åtgärd för att eliminera orsaken till en *avvikelse* (3.47) och för att förebygga upprepning av denna

3.18
härlett mått
mått (3.42) som definieras som en funktion av två eller fler *basmått* (3.8)

[KÄLLA: ISO/IEC/IEEE 15939:2017, 3.8, modifierad – Anm. 1 till termpost har tagits bort.]

3.19
dokumenterad information
information som ska styras och underhållas av en *organisation* (3.47) samt det medium på vilket informationen finns

Anm. 1 till termpost: Dokumenterad information kan ha vilket format som helst, finnas på vilket medium som helst och ha vilken källa som helst.

Anm. 2 till termpost: Dokumenterad information kan avse t.ex.

– ledningssystemet, inklusive tillhörande processer

– information som skapats så att organisationens verksamhet kan fungera (styrande dokument)