# SVENSK STANDARD
# SS-EN ISO/IEC 27001:2017

**Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav (ISO/IEC 27001:2013 med Cor 1:2014 and Cor 2:2015)**

**Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015)**

Svenska Institutet för Standarder

Språk: svenska/Swedish, engelska/English

Utgåva: 1

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: 2017-02-28
ICS: 01.140.30;03.100.70;04.050;33.040.40;35.020;35.030;35.040;35.080

Svenska Institutet för Standarder

Den internationella standarden ISO/IEC 27001:2017 gäller som svensk standard. Detta dokument innehåller den svenska språkversionen av ISO/IEC 27001:2017 följd av den officiella engelska språkversionen.

Denna standard ersätter SS-ISO/IEC 27001:2014, utgåva 2 och SS-ISO /IEC 27001:2014/Cor 2:2016, utgåva 1.

The International Standard ISO/IEC 27001:2017 has the status of a Swedish Standard. This document contains the Swedish language version of ISO/IEC 27001:2017 followed by the official English version.

This standard supersedes the Swedish Standard SS-ISO/IEC 27001:2014, edition 2 and SS-ISO/IEC 27001:2014/Cor 2:2016, edition 1.

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

# EN ISO/IEC 27001

February 2017

ICS 03.100.70; 35.030

Svensk version

# Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013 med Cor 1:2014 och Cor 2:2015)

Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences (ISO/IEC 27001:2013 y compris Cor 1:2014 et Cor 2:2015)

Informationstechnik - Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015)

Denna standard är den officiella svenska versionen av EN ISO/IEC 27001:2016 med Cor 1:2014 och Cor 2:2015. För översättningen står SIS.

Denna Europastandard antogs av CEN och CENELEC den 26 januari 2017.

CEN och CENELECs medlemmar är förpliktade att följa fordringarna i CEN/CENELECs interna bestämmelser som anger på vilka villkor denna Europastandard i oförändrat skick skall ges status som nationell standard. Aktuella förteckningar och bibliografiska referenser rörande sådana nationella standarder kan på begäran erhållas från CENs centralsekretariat eller från någon av CENs eller CENELECs medlemmar.

Denna Europastandard finns i tre officiella versioner (engelsk, fransk och tysk). En version på något annat språk, översatt under ansvar av en CEN eller CENELEC-medlem till sitt eget språk och anmäld till CENs centralsekretariat, har samma status som de officiella versionerna.

CENs och CENELECs medlemmar är de nationella standardiseringsorganen och nationalkommittéerna i, Belgien, Bulgarien, , Cypern, Danmark, Estland, Finland, Frankrike, Grekland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, före detta jugoslaviska republiken Makedonien, Malta, Nederländerna, Norge, Polen, Portugal, Rumänien, Schweiz, Serbien, Slovakien, Slovenien, Spanien, Storbritannien, Sverige, Tjeckien, Turkiet, Tyskland, Ungern, och Österrike.

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

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



Ref. No. EN ISO/IEC 27001:2017 E

## Innehåll

# Europeiska förordet

Detta dokument ISO/IEC 27001:2013 med Cor 1:2014 och Cor 2:2015 har utarbetats av den tekniska kommittén ISO/IEC JTC 1 “Information technology” av the InternationalOrganization for Standardization (ISO) och the International Electrotechnical Commission (IEC) och har antagits som EN ISO/IEC 27001:2017.

Denna Europastandard ska ges status av nationell standard, antingen genom publicering av en identisk text eller genom ikraftsättning senast augusti 2017, och motstridande nationella standarder ska upphävas senast augusti 2017.

Det bör uppmärksammas att vissa beståndsdelar i denna Europastandard möjligen kan vara föremål för patenträtter. CEN och/eller CENELEC ska inte hållas ansvariga för att identifiera någon eller alla sådana patenträtter.

Enligt CEN/CENELECs interna bestämmelser ska följande länder fastställa denna Europastandard: Belgien, Bulgarien, , Cypern, Danmark, Estland, Finland, Frankrike, Grekland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, före detta jugoslaviska republiken Makedonien, Malta, Nederländerna, Norge, Polen, Portugal, Rumänien, Schweiz, Serbien, Slovakien, Slovenien, Spanien, Storbritannien, Sverige, Tjeckien, Turkiet, Tyskland, Ungern, och Österrike.

## Ikraftsättningsnotering

Texten i den internationella standarden ISO/IEC 27001:2013 med Cor 1:2014 och Cor 2:2015 har godkänts av CEN as EN ISO/IEC 27001:2017 utan någon ändring.

# 0 Orientering

## 0.1 Allmänt

Denna standard har tagits fram för att tillhandahålla krav för att upprätta, införa, underhålla och ständigt förbättra ett ledningssystem för informationssäkerhet. Antagandet av ett ledningssystem för informationssäkerhet är ett strategiskt beslut för en organisation. Upprättandet och införandet av en organisations ledningssystem för informationssäkerhet påverkas av organisationens behov och mål, säkerhetskrav, de organisatoriska processer som används och organisationens storlek och struktur. Alla dessa påverkande faktorer kan komma att förändras över tiden.

Ledningssystemet för informationssäkerhet bevarar informationens konfidentialitet, riktighet och tillgänglighet genom att tillämpa en riskhanteringsprocess och ger förtroende för berörda parter att risker hanteras på ett adekvat sätt.

Det är viktigt att ledningssystemet för informationssäkerhet är en integrerad del av organisationens processer och övergripande ledningsstruktur och att informationssäkerhet beaktas i utformningen av processer, informationssystem och säkerhetsåtgärder. Det förväntas att ett införande av ett ledningssystem för informationssäkerhet sker i en omfattning som anpassas till organisationens behov.

Denna standard kan användas internt och av externa parter för att bedöma organisationens förmåga att uppfylla organisationens egna informationssäkerhetskrav.

Den ordning i vilken kraven presenteras i denna standard syftar inte till att återspegla deras betydelse och antyder heller inte den ordning i vilken de ska genomföras. De redovisade kraven numreras enbart i hänvisningssyfte.

SS-ISO/IEC 27000 beskriver en översikt av och vokabulär för ledningssystem för informationssäkerhet, med referens till standardserien som relaterar till ledningssystem för informationssäkerhet (inklusive SS-ISO/IEC 27003 [2], SS-ISO/IEC 27004 [3] och SS-ISO/IEC 27005 [4]), med relaterade termer och definitioner.

## 0.2 Kompatibilitet med andra ledningssystemstandarder

Denna standard tillämpar högnivåstruktur, identiska titlar på underavsnitt, identisk text, vanliga termer och grundbegrepp som de definierats i bilaga SL av del 1 av ISO/IEC direktiven, konsoliderade ISO-tillägg, och är därför kompatibel med andra ledningssystemstandarder som har antagit bilaga SL.

Detta gemensamma angreppssätt, som definierats i bilaga SL, kommer att vara användbart för de organisationer som väljer att använda ett enda ledningssystem som uppfyller kraven i två eller flera ledningssystemstandarder.

# Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav

## 1 Omfattning

Denna standard specificerar kraven för upprättande, införande, underhåll och ständig förbättring av ett ledningssystem för informationssäkerhet inom ramarna för organisationen. Denna standard innehåller också krav på bedömning och behandling av informationssäkerhetsrisker, anpassat till organisationens behov. Kraven som anges i denna standard är generiska och är avsedda att vara tillämpliga i alla organisationer, oavsett typ, storlek och slag. Att undanta något av kraven specificerade i avsnitt 4 till 10 är inte acceptabelt när en organisation avser efterleva denna standard.

## 2 Normativa hänvisningar

Detta dokument hänvisar till följande dokument som är nödvändiga när detta dokument ska tillämpas. För daterade hänvisningar gäller endast den utgåva som anges. För odaterade hänvisningar gäller senaste utgåvan av dokumentet (inklusive alla tillägg).

SS-ISO/IEC 27000, *Informationsteknologi — Säkerhetstekniker — Ledningssystem för informationssäkerhet — Översikt och terminologi*

## 3 Termer och definitioner

För tillämpningen av detta dokument gäller de termer och definitioner som anges i SS-ISO/IEC 27000.

## 4 Organisationens förutsättningar

### 4.1 Att förstå organisationen och dess förutsättningar

Organisationen ska avgöra vilka externa och interna frågor som är relevanta för dess syfte och som påverkar dess förmåga att nå de avsedda resultaten med sitt ledningssystem för informationssäkerhet.

ANM. Fastställandet av dessa frågor avser upprättande av organisationens externa och interna kontext vilka beaktas i avsnitt 5.3 i SS-ISO 31000:2009 [5].

### 4.2 Att förstå intressenters behov och förväntningar

Organisationen ska bestämma:

a) vilka intressenter som är relevanta för ledningssystemet för informationssäkerhet; och

b) dessa intressenters krav som är relevanta för informationssäkerhet.

ANM. Berörda parters krav kan inkludera rättsliga och regelmässiga krav och avtalsförpliktelser.

### 4.3 Att bestämma ledningssystemets omfattning

Organisationen ska bestämma avgränsningar och tillämpligheten av ledningssystemet för informationssäkerhet för att fastställa systemets omfattning.

När organisationen bestämmer denna omfattning ska den beakta:

a) de interna och externa frågor som det hänvisas till i 4.1;

b) de krav som det hänvisas till i 4.2; och

c) gränssnitt och beroenden mellan aktiviteter som utförs av organisationen, och de som utförs av andra organisationer.

Omfattningen ska finnas tillgänglig som dokumenterad information.

### 4.4 Ledningssystem för informationssäkerhet

Organisationen ska upprätta, införa, underhålla och ständigt förbättra ett ledningssystem för informationssäkerhet, inklusive nödvändiga processer och deras samverkan, enligt kraven i denna standard.

## 5 Ledarskap

### 5.1 Ledarskap och engagemang

Högsta ledningen ska tydligt visa ledarskap och åtagande i fråga om ledningssystemet för informationssäkerhet genom att:

a) säkerställa att informationssäkerhetspolicy och informationssäkerhetsmål är upprättade och är förenliga med organisationens strategiska inriktning;

b) säkerställa att kraven i ledningssystemet för informationssäkerhet integreras i organisationens verksamhetsprocesser;

c) säkerställa att ledningssystemet för informationssäkerhet ges nödvändiga resurser;

d) kommunicera betydelsen av att systemet för informationssäkerhet leds och styrs på ett väl fungerande sätt och att kraven i ledningssystemet för informationssäkerhet uppfylls;

e) säkerställa att ledningssystemet för informationssäkerhet uppnår avsett resultat;

f) leda och stödja personer så att de bidrar till ett väl fungerande ledningssystem för informationssäkerhet;

g) främja ständig förbättring; och

h) ge stöd till andra relevanta ledande befattningshavare så att de tydligt utövar sitt ledarskap på ett sätt som är lämpligt inom deras ansvarsområden.

ANM. Begreppet ”verksamhet” i denna standard bör tolkas i vid bemärkelse att avse de aktiviteter som är av central betydelse för syftet med organisationens existens.

### 5.2 Policy

Högsta ledningen ska upprätta en informationssäkerhetspolicy som:

a) är anpassad till organisationens syfte;

b) ger ett ramverk för att sätta informationssäkerhetsmål;

c) innefattar ett åtagande att uppfylla tillämpliga krav relaterade till informationssäkerhet; och

d) innefattar ett åtagande att ständigt förbättra ledningssystemet för informationssäkerhet.

Informationssäkerhetspolicyn ska:

e) finnas tillgänglig i dokumenterad form;

f) kommuniceras inom organisationen; och

g) i tillämplig utsträckning vara tillgänglig för intressenter.

### 5.3 Befattningar, ansvar och befogenheter inom organisationen

Högsta ledningen ska säkerställa att relevanta befattningar har tilldelats ansvar och befogenheter och att dessa är kommunicerade inom organisationen.

Högsta ledningen ska tilldela ansvar och befogenhet för att:

a) säkerställa att ledningssystemet för informationssäkerhet uppfyller kraven i denna standard; och

b) rapportera till högsta ledningen om hur ledningssystemet för informationssäkerhet fungerar.

ANM. Högsta ledningen kan också tilldela ansvar och befogenheter inom organisationen för rapportering av status avseende ledningssystemet för informationssäkerhet.

## 6 Planering

### 6.1 Åtgärder för att hantera risker och möjligheter

#### 6.1.1 Allmänt

När organisationen planerar ledningssystemet för informationssäkerhet ska den beakta de frågor som hänvisas till i 4.1 och de krav som hänvisas till i 4.2 samt avgöra vilka risker och möjligheter som behöver hanteras för att

a) säkra att ledningssystemet för informationssäkerhet kan ge avsett resultat;

b) förebygga eller minska oönskade effekter; och

c) uppnå ständig förbättring.

Organisationen ska planera:

d) åtgärder för att hantera dessa risker och möjligheter; och

e) hur den ska

1) integrera och införa åtgärderna i processerna inom sitt ledningssystem för informationssäkerhet;

2) utvärdera om åtgärderna har gett avsedd verkan.

#### 6.1.2 Bedömning av informationssäkerhetsrisker

Organisationen ska fastställa och tillämpa en process för bedömning av informationssäkerhetsrisker som:

a) upprättar och underhåller kriterier för informationssäkerhetsrisker som inkluderar:

1) kriterier för riskacceptans; och

2) kriterier för bedömningar av informationssäkerhetsrisker;

b) säkerställer att upprepade bedömningar av informationssäkerhetsrisker genererar konsistenta, korrekta och jämförbara resultat;