SVENSK STANDARD
SS-ISO/IEC 27001:2014

Fastställd/Approved: 2014-02-26
Publicerad/Published: 2014-02-27
Utgåva/Edition: 2
Språk/Language: svenska/Swedish; engelska/English
ICS: 01.140.30; 04.050; 33.040.40; 35.020; 35.040; 35.080

Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav
(ISO/IEC 27001:2013, IDT)

Information technology – Security techniques – Information security management systems – Requirements
(ISO/IEC 27001:2013, IDT)

Standarder får världen att fungera

SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiviserar din verksamhet.

Delta och påverka
Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

Ta del av det färdiga arbetet
Vi erbjuder våra kunder allt som rör standarder och deras tillämpning. Hos oss kan du köpa alla publikationer du behöver – allt från enskilda standarder, tekniska rapporter och standard-paket till handböcker och onlinetjänster. Genom vår webbtjänst e-nav får du tillgång till ett lättnavigerat bibliotek där alla standarder som är aktuella för ditt företag finns tillgängliga. Standarder och handböcker är källor till kunskap. Vi säljer dem.

Utveckla din kompetens och lyckas bättre i ditt arbete
Hos SIS kan du gå öppna eller företagsinterna utbildningar kring innehåll och tillämpning av standarder. Genom vår närhet till den internationella utvecklingen och ISO får du rätt kunskap i rätt tid, direkt från källan. Med vår kunskap om standarders möjligheter hjälper vi våra kunder att skapa verklig nytta och lönsamhet i sina verksamheter.

Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på www.sis.se eller ta kontakt med oss på tel 08-555 523 00.

Standards make the world go round

SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.

Take part and have influence
As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

Get to know the finished work
We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

Increase understanding and improve perception
With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

If you want to know more about SIS, or how standards can streamline your organisation, please visit www.sis.se or contact us on phone +46 (0)8-555 523 00

Den internationella standarden ISO/IEC 27001:2013 gäller som svensk standard. Detta dokument innehåller den svenska språkversionen av ISO/IEC 27001:2013 följd av den officiella engelska språkversionen.

Denna standard ersätter SS-ISO/IEC 27001:2006 utgåva 1.

The International Standard ISO/IEC 27001:2013 has the status of a Swedish Standard. This document contains the Swedish language version of ISO/IEC 27001:2013 followed by the official English version.

This standard supersedes the Swedish Standard SS-ISO/IEC 27001:2006, edition 1.

Upplysningar om sakinnehållet i standarden lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00. Standarder kan beställas hos SIS Förlag AB som även lämnar allmänna upplysningar om svensk och utländsk standard.

Information about the content of the standard is available from the Swedish Standards Institute (SIS), telephone +46 8 555 520 00. Standards may be ordered from SIS Förlag AB, who can also provide general information about Swedish and foreign standards.

Standarden är framtagen av kommittén för 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.

Innehåll

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 direktiven, del 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.

SS-ISO/IEC 27001 har tagits fram av den gemensamma tekniska kommittén ISO/IEC JTC 1, Informationsteknologi, underkommitté SC 27, IT-säkerhetstekniker.

Denna andra upplaga utgåvan och ersätter den första utgåvan (SS-ISO/IEC 27001:2006), efter teknisk revidering.

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;

c) identifierar informationssäkerhetsriskerna genom att:

1) tillämpa processen för bedömning av informationssäkerhetsrisker för att identifiera risker förknippade med förlust av konfidentialitet, riktighet och tillgänglighet inom omfattningen för ledningssystemet för informationssäkerhet; och

2) identifiera ägare till riskerna;

d) analyserar informationssäkerhetsriskerna genom att:

1) bedöma de potentiella konsekvenser som skulle uppstå om riskerna som identifierats i 6.1.2 c) 1) realiseras;

2) bedöma den realistiska sannolikheten för förekomsten av de risker som identifierats i 6.1.2 c) 1); och

3) fastställa risknivåer;

e) utvärderar informationssäkerhetsriskerna:

1) jämför resultaten av riskanalyser med riskkriterierna fastställda i 6.1.2 a); och

2) prioriterar de analyserade riskerna för riskbehandling.

Organisationen ska bevara dokumenterad information om processen för bedömning av informationssäkerhetsrisker.

6.1.3 Behandling av informationssäkerhetsrisker

Organisationen ska fastställa och tillämpa en process för behandling av informationssäkerhetsrisker för att:

a) välja ut lämpliga alternativ för behandling av informationssäkerhetsrisker, med hänsyn tagen till resultaten av riskbedömningen;

b) fastställa alla säkerhetsåtgärder som är nödvändiga för att införa valda alternativ för behandling av informationssäkerhetsrisker;

ANM. Organisationer kan utforma säkerhetsåtgärder efter behov, eller identifiera dem från någon annan källa.

c) jämföra säkerhetsåtgärderna fastställda i 6.1.3 b) ovan med de i bilaga A och verifiera att inga nödvändiga säkerhetsåtgärder har utelämnats;

ANM. 1 Bilaga A innehåller en omfattande lista över åtgärdsmål och säkerhetsåtgärder. Användare av denna internationella standard hänvisas till bilaga A för att säkerställa att inga nödvändiga säkerhetsåtgärder förbises.

ANM. 2 Åtgärdsmål ingår implicit i valda säkerhetsåtgärder. Åtgärdsmålen och säkerhetsåtgärderna förtecknade i bilaga A är inte uttömmande och ytterligare åtgärdsmål och säkerhetsåtgärder kan behövas.

d) skapa ett uttalande om tillämplighet som innehåller de nödvändiga säkerhetsåtgärderna (se 6.1.3 b) och c)) och motivering för inkludering, om de är införda eller inte, och motivering för uteslutning av säkerhetsåtgärder från bilaga A;

e) formulera en plan för behandling av informationssäkerhetsrisker; och

f) utverka riskägarnas godkännande av riskbehandlingsplanen för informationssäkerhet, samt deras godkännande av de kvarvarande informationssäkerhetsriskerna.

Organisationen ska bevara dokumenterad information om processen för behandling av informationssäkerhetsrisker.

ANM. Processen för bedömningen och behandling av informationssäkerhetsrisker i denna internationella standard överensstämmer med de principer och allmänna riktlinjer föreskrivna i SS-ISO 31000 [5].

6.2 Informationssäkerhetsmål och planering för att uppnå dem

Organisationen ska upprätta informationssäkerhetsmål för relevanta funktioner och nivåer.

Informationssäkerhetsmålen ska:

a) stå i överensstämmelse med informationssäkerhetspolicyn;

b) vara mätbara (om det är praktiskt möjligt);

c) beakta tillämpliga informationssäkerhetskrav, och resultat från riskbedömning och riskbehandling;

d) kommuniceras; och

e) uppdateras efter behov.

Organisationen ska bevara dokumenterad information om informationssäkerhetsmålen.

När organisationen planerar för att uppnå sina informationssäkerhetsmål ska den avgöra:

f) vad som ska göras;

g) vilka resurser som kommer att krävas;

h) vem som ska ansvara;

i) när det ska vara genomfört; och

j) hur resultaten ska utvärderas.

7 Stöd

7.1 Resurser

Organisationen ska fastställa vilka resurser som behövs för att upprätta, införa, underhålla och ständigt förbättra sitt ledningssystem för informationssäkerhet. Organisationen ska även tillhandahålla dessa resurser.

7.2 Kompetens

Organisationen ska:

a) avgöra vilken kompetens som är nödvändig hos den eller de personer som arbetar åt den och som påverkar dess informationssäkerhetsprestanda;

b) säkerställa att dessa personer är kompetenta, baserat på lämplig utbildning, upplärning eller erfarenhet;

c) där så är tillämpligt, vidta åtgärder för att införskaffa den nödvändiga kompetensen och utvärdera verkan av de vidtagna åtgärderna; och

d) bevara lämplig dokumenterad information som belägg för kompetens.

ANM. Tillämpliga åtgärder kan exempelvis vara att ge anställda möjlighet att få upplärning, mentor, eller andra arbetsuppgifter, eller att hyra in eller anlita kompetenta personer.

7.3 Medvetenhet

Personer som arbetar inom eller åt organisationen ska vara medvetna om:

a) informationssäkerhetspolicyn;