SVENSK STANDARD
SS-EN ISO 22301:2014

Fastställd/Approved: 2014-07-27
Publicerad/Published: 2014-09-10
Utgåva/Edition: 1
Språk/Language: svenska/Swedish; engelska/English
ICS: 03.100.01; 04.140

Samhällssäkerhet – Ledningssystem för kontinuitet – Krav (ISO 22301:2012)

Societal security – Business continuity management systems – Requirements (ISO 22301:2012)

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-102515

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-102515

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

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-102515

Europastandarden EN ISO 22301:2014 gäller som svensk standard. Detta dokument innehåller den officiella svenska/engelska versionen av EN ISO 22301:2014.

Denna standard ersätter SS-ISO 22301:2012, utgåva 1.

The European Standard EN ISO 22301:2014 has the status of a Swedish Standard. This document contains the official version of EN ISO 22301:2014.

This standard supersedes the Swedish Standard SS-ISO 22301:2012, edition 1.

I denna standard är ändringar enligt *ISO 22301:2012, Corrected version 2014-06-15* inarbetade.

The corrections in *ISO 22301:2012, Corrected version 2014-06-15* are incorporated in this standard.

© Copyright/Upphovsrätten till denna produkt tillhör SIS, Swedish Standards Institute, Stockholm, Sverige. Användningen av denna produkt regleras av slutanvändarlicensen som återfinns i denna produkt, se standardens sista sidor.

© Copyright SIS, Swedish Standards Institute, Stockholm, Sweden. All rights reserved. The use of this product is governed by the end-user licence for this product. You will find the licence in the end of this document.

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.

Denna standard är framtagen av kommittén för Samhällssäkerhet, SIS/TK 494.

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.

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-102515

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-102515

EUROPASTANDARD
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO 22301

Juli 2014

ICS 03.100.01

Samhällssäkerhet - Ledningssystem för kontinuitet - Krav (ISO 22301:2012)

Sécurité sociétale - Systèmes de management de la continuité d'activité - Exigences (ISO 22301:2012)

Societal security - Business continuity management systems - Requirements (ISO 22301:2012)

Sicherheit und Schutz des Gemeinwesens - Aufrechterhaltung der Betriebsfähigkeit - Anforderungen (ISO 22301:2012)

Denna standard är den officiella svenska versionen av EN ISO 22301:2014. För översättningen svarar SIS.

Denna Europastandard antogs av CEN den 17 Juli 2014.

CEN-medlemmarna är förpliktade att följa fordringarna i CEN/CENELECs interna bestämmelser som anger på vilka villkor denna Europastandard i oförändrat skick ska 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 medlemmar.

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

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

CEN

European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

Management Centre: Avenue Marnix 17, B-1000 BRUSSELS

© 2014 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-102515

Innehåll

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-102515

Förord

Texten till den internationella standarden ISO 22301:2012, har utarbetats av den tekniska kommittén ISO/TC 223 *Societal security*, och har överförts till EN ISO 22301:2014 av den tekniska kommittén CEN/TC 391 *Societal and citizen security*. Sekretariatet hålls av NEN.

Denna Europastandard ska ges status av nationell standard, antingen genom publicering av en identisk text eller genom ikraftsättning senast januari 2015, och motstridande nationella standarder ska upphävas senast januari 2015.

Det bör uppmärksammas att vissa beståndsdelar i denna Europastandard möjligen kan vara föremål för patenträtter. CEN ska inte hållas ansvarig 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, Makedonien, Malta, Nederländerna, Norge, Polen, Portugal, Rumänien, Schweiz, Slovakien, Slovenien, Spanien, Storbritannien, Sverige, Tjeckien, Turkiet, Tyskland, Ungern och Österrike.

Ikraftsättningsnotering

Texten i den internationella standarden ISO 22301:2012 har godkänts av CEN som Europastandard utan någon ändring.

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-102515

0 Orientering

0.1 Allmänt

Denna standard anger krav på att upprätta och tillämpa ett effektivt ledningssystem för kontinuitet.

I ett sådant system framhålls vikten av att

— förstå organisationens behov och nödvändigheten av att upprätta policy och mål för kontinuitet,

— införa och tillämpa styrning och metoder för att sköta en organisations övergripande förmåga att hantera avbrott,

— övervaka och granska prestanda och verkan hos ledningssystemet,

— ständigt förbättra, grundat på objektiv mätning.

Ett ledningssystem för kontinuitet har liksom andra ledningssystem följande huvuddelar:

a) en policy;

b) personer med definierade ansvar;

c) ledningsprocesser för

   1) policy,

   2) planering,

   3) införande och tillämpning,

   4) bedömning av prestanda,

   5) ledningens genomgång,

   6) förbättring.

d) dokumentation som ger reviderbara belägg;

e) andra processer för kontinuitetshantering som är relevanta för organisationen.

Kontinuitet bidrar till ett mindre sårbart samhälle. Samhället i stort och inverkan av organisationens omgivning på organisationen medför att andra organisationer kan behöva bli involverade i återhämtningsprocessen.

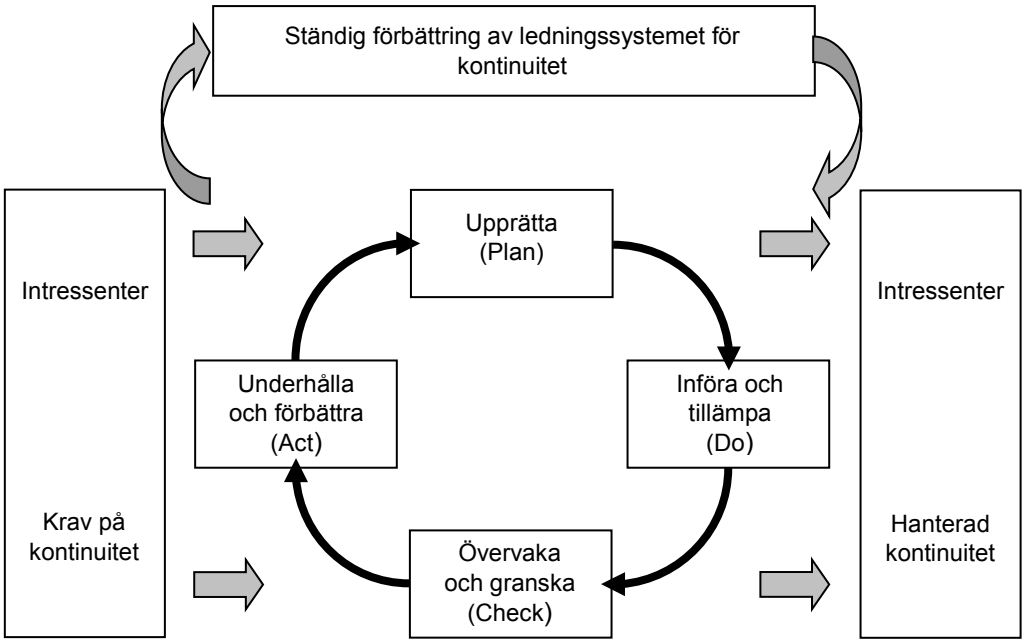
0.2 Plan-Do-Check-Act (PDCA)-modellen

Denna standard tillämpar Plan-Do-Check-Act (PDCA)-modellen för att planera, upprätta, införa, tillämpa, övervaka, granska, underhålla och ständigt förbättra verkan hos en organisations ledningssystem för kontinuitet.

Detta säkerställer en viss samstämmighet med andra standarder för ledningssystem, bl.a. ISO 9001, *Kvalitetsledningssystem*, ISO 14001, *Miljöledningssystem*, ISO/IEC 27001, *Ledningssystem för informationssäkerhet*, ISO/IEC 20000-1, *Informationsteknik — Ledningssystem för tjänster* och ISO 28000, *Specification for security management system for the supply chain*, och stöder att systemet införs och tillämpas enhetligt och kan integreras med andra ledningssystem.

Figur 1 visar hur ett ledningssystem för kontinuitet har intressenter och krav på kontinuitet som insatser och med hjälp av nödvändiga åtgärder och processer åstadkommer resultat (dvs. styrd kontinuitet) som uppfyller dessa krav.

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-102515



Figur 1 — PDCA-modellen tillämpad på processer för kontinuitetshantering

Tabell 1 — Förklaring till PDCA-modellen

Plan (Upprätta)	Upprätta policy, övergripande och detaljerade mål, styrmedel, processer och rutiner relevanta för förbättring av kontinuiteten i avsikt att åstadkomma resultat som är i linje med organisationens övergripande policyer och mål.
Do (Införa och tillämpa)	Införa och tillämpa policy, styrmedel, processer och rutiner för kontinuitet.
Check (Övervaka och granska)	Övervaka och granska prestanda mot policy och mål för kontinuitet, rapportera resultaten till ledningens genomgång samt besluta och godkänna åtgärder för avhjälpande och förbättring.
Act (Underhålla och förbättra)	Underhålla och förbättra ledningssystemet för kontinuitet genom att vidta korrigerande åtgärder, baserade på ledningens genomgång och förnyad bedömning av ledningssystemets omfattning samt på policy och mål för kontinuitet.

Svensk ANM. I denna standard används termen ”ledningssystem” som synonym till ”ledningssystem för kontinuitet”.

0.3 Delar av PDCA i denna standard

I den Plan-Do-Check-Act-modell som visas i figur 1 täcker avsnitten 4 t.o.m. 10 i denna standard följande delar:

— Avsnitt 4 är en del av ”Plan”. Avsnittet beskriver villkor som är nödvändiga för att bestämma förutsättningarna för organisationens ledningssystem för kontinuitet liksom behov, krav och omfattning.

— Avsnitt 5 är en del av ”Plan”. Det sammanfattar de krav som rör högsta ledningens roll i fråga om ledningssystemet och anger hur ledningen uttrycker sina förväntningar till organisationen i ett policyuttalande.

— Avsnitt 6 är en del av ”Plan”. Avsnittet anger krav när det gäller att upprätta strategiska mål och vägledande principer för ledningssystemet i sin helhet. Innehållet i avsnitt 6 skiljer sig från den behandling av risker som kommer från riskbedömning liksom återställningsmål härledda från konsekvensanalyser.

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-102515

ANM. Processkrav på konsekvensanalys och riskbedömning beskrivs närmare i avsnitt 8.

— Avsnitt 7 är en del av ”Plan”. Det behandlar stöd för tillämpningen av ledningssystemet i fråga om anskaffning av kompetens och om återkommande/behovsstyrd kommunikation med intressenter. I detta ingår att upprätta, styra, underhålla och bevara den dokumentation som krävs.

— Avsnitt 8 behandlar ”Do”. Detta avsnitt definierar krav på kontinuitet, ger anvisning om hur de ska behandlas och vad som ska ingå i rutiner för att hantera avbrott.

— Avsnitt 9 behandlar ”Check”. Det sammanfattar de krav som är nödvändiga för att mäta prestanda hos kontinuitetshanteringen, hur väl ledningssystemet uppfyller kraven i denna standard och ledningens förväntningar samt söker återföring från ledningen i fråga om förväntningar.

— Avsnitt 10 behandlar ”Act”. Avvikelser inom ledningssystemets ram identifieras och behandlas genom korrigerande åtgärder.

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-102515

Samhällssäkerhet — Ledningssystem för kontinuitet — Krav

1 Omfattning

Denna standard för ledning av kontinuitet anger krav för att planera, upprätta, införa, tillämpa, övervaka, underhålla och ständigt förbättra ett dokumenterat ledningssystem för att skydda mot, minska sannolikheten och förbereda för, agera på och återställa efter avbrott, när de inträffar.

Kraven i denna standard är allmänna och avsedda att vara tillämpbara för varje organisation eller delar av en sådan, oavsett typ, storlek och inriktning. I vilken utsträckning dessa krav är tillämpbara är beroende av organisationens komplexitet och verksamhetsomgivning.

Avsikten med denna standard är inte att tvinga fram en likformig uppbyggnad hos ledningssystem för kontinuitet, utan att hjälpa en organisation att utforma ett ledningssystem som passar för dess behov och som uppfyller dess intressenters krav. Behoven baseras på krav i författningar, organisatoriska krav och branschkrav, på varor och tjänster, på tillämpade processer, på organisationens storlek och uppbyggnad och på intressenternas krav.

Denna standard är tillämpbar för alla organisationer oavsett storlek och inriktning som vill

a) upprätta, införa, underhålla och förbättra ett ledningssystem för kontinuitet,

b) säkerställa att en fastställd kontinuitetspolicy följs,

c) visa inför andra att organisationen arbetar efter standarden,

d) söka certifiering av sitt ledningssystem från ett ackrediterat certifieringsorgan, eller

e) göra en egenbedömning och egen förklaring av överensstämmelse med denna standard.

Denna standard kan användas för att bedöma en organisations förmåga att uppfylla dess egna behov och förpliktelser i fråga om kontinuitetshantering.

2 Normativa hänvisningar

Detta dokument hänvisar till följande dokument som är absolut 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).

Inga normativa hänvisningar ges.

3 Termer och definitioner

För tillämpning av detta dokument gäller de termer och definitioner som följer nedan.

3.1
verksamhet
process eller grupp av processer, utförd av organisationen (eller för dess räkning), som åstadkommer eller stöder en eller flera varor och tjänster

EXEMPEL Sådana processer är bl.a. ekonomi, telefonförsäljning, IT, tillverkning, distribution.