

SVENSK STANDARD

SS 22304:2023

**Säkerhet och resiliens – Ledningssystem för
kontinuitetshantering – Handbok för kontinuitetshantering enligt
SS-EN ISO 22301**

**Security and resilience – Business continuity management
systems – Handbook for Business continuity management in
accordance with SS-EN ISO 22301**



SIS Svenska
Institutet för
Standarder

Språk: svenska/Swedish

Utgåva: 2

**SIS single user license: Myndigheten För Samhällsskydd och
Beredskap (MSB) Ordered by:
Emma.johansson@energiforetagen.se. Date: 2024-01-10**

**This standard is prepaid by Myndigheten för samhällsskydd och
beredskap (MSB).**

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](https://www.sis.se) eller ring 08 - 555 523 10

© Copyright/Upphovsrätten till denna produkt tillhör Svenska institutet för standarder, Stockholm, Sverige. Upphovsrätten och användningen av denna produkt regleras i slutanvändarlicensen som återfinns på [sis.se/slutanvandarlicens](https://www.sis.se/slutanvandarlicens) och som du automatiskt blir bunden av när du använder produkten. För ordlista och förkortningar se [sis.se/ordlista](https://www.sis.se/ordlista).

© Copyright Svenska institutet för standarder, Stockholm, Sweden. All rights reserved. The copyright and use of this product is governed by the end-user licence agreement which you automatically will be bound to when using the product. You will find the licence at [sis.se/enduserlicenseagreement](https://www.sis.se/enduserlicenseagreement).

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 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.

Denna standard ersätter SS 22304:2014, utgåva 1.

This standard supersedes the Swedish Standard SS 22304:2014, edition 1.

LÄSANVISNINGAR FÖR STANDARDER

I dessa anvisningar behandlas huvudprinciperna för hur regler och yttre begränsningar anges i standardiseringsprodukter.

Krav

Ett krav är ett uttryck i ett dokumentets innehåll som anger objektivt verifierbara kriterier som ska uppfyllas och från vilka ingen avvikelse tillåts om efterlevnad av dokumentet ska kunna åberopas. Krav uttrycks med hjälpverbet **ska** (eller **ska inte** för förbud).

Rekommendation

En rekommendation är ett uttryck i ett dokumentets innehåll som anger en valmöjlighet eller ett tillvägagångssätt som bedöms vara särskilt lämpligt utan att nödvändigtvis nämna eller utesluta andra. Rekommendationer uttrycks med hjälpverbet **bör** (eller **bör inte** för avrådanden).

Instruktion

Instruktioner anges i imperativ form och används för att ange hur något görs eller utförs. De kan underordnas en annan regel, såsom ett krav eller en rekommendation. De kan även användas självständigt, och är då att betrakta som krav.

Förklaring

En förklaring är ett uttryck i ett dokumentets innehåll som förmedlar information. En förklaring kan uttrycka tillåtelse, möjlighet eller förmåga. Tillåtelse uttrycks med hjälpverbet **får** (eller motsatsen **behöver inte**). Möjlighet och förmåga uttrycks med hjälpverbet **kan** (eller motsatsen **kan inte**).

READING INSTRUCTIONS FOR STANDARDS

These instructions cover the main principles for the use of provisions and external constraints in standardization deliverables.

Requirement

A requirement is an expression, in the content of a document, that conveys objectively verifiable criteria to be fulfilled, and from which no deviation is permitted if conformance with the document is to be claimed. Requirements are expressed by the auxiliary **shall** (or **shall not** for prohibition).

Recommendation

A recommendation is an expression, in the content of a document, that conveys a suggested possible choice or course of action deemed to be particularly suitable, without necessarily mentioning or excluding others. Recommendations are expressed by the auxiliary **should** (or **should not** for dissuasion).

Instruction

An instruction is expressed in the imperative mood and is used in order to convey an action to be performed. It can be subordinated to another provision, such as a requirement or a recommendation. It can also be used independently and is then to be regarded as a requirement.

Statement

A statement is an expression, in the content of a document, that conveys information. A statement can express permission, possibility or capability. Permission is expressed by the auxiliary **may** (its opposite being **need not**). Possibility and capability are expressed by the auxiliary **can** (its opposite being **cannot**).

Innehållsförteckning

Inledning.....	iii
0.1 Bakgrund och syfte	iii
0.2 Koppling till standardisering inom CEN och ISO.....	viii
0.3 Koppling till lagstiftning.....	viii
0.4 Väsentliga skillnader mot föregående utgåva	viii
1 Omfattning.....	1
2 Normativa hänvisningar.....	1
3 Termer och definitioner	1
4 Organisationens förutsättningar.....	4
4.1 Att förstå organisationen och dess förutsättningar.....	4
4.2 Att förstå berörda parter och behov och förväntningar	5
4.3 Att bestämma ledningssystemets omfattning	6
4.4 Ledningssystem för kontinuitetshantering.....	7
5 Ledarskap	7
5.1 Ledarskap och åtagande.....	7
5.2 Policy	8
5.3 Roller, ansvar och befogenheter.....	9
6 Planering.....	10
6.1 Åtgärder för att hantera risker och möjligheter.....	10
6.2 Kontinuitetsmål och planering för att uppnå dem	11
6.3 Planering av förändring.....	12
7 Stöd.....	13
7.1 Resurser.....	13
7.2 Kompetens.....	13
7.3 Medvetenhet	14
7.4 Kommunikation.....	14
7.5 Dokumenterad information.....	14
8 Verksamhet	15
8.1 Planering och styrning av verksamheten.....	15
8.2 Konsekvensanalys och riskbedömning.....	17
8.3 Kontinuitetsstrategier och lösningar	25
8.4 Kontinuitetsplaner och rutiner.....	31
8.5 Övningsprogram.....	37
8.6 Utvärdering av dokumentation och förmågor för kontinuitet.....	38
9 Utvärdering av prestanda	40
9.1 Övervakning, mätning, analys och utvärdering	40
9.2 Intern revision	41
9.3 Ledningens genomgång	43
10 Förbättringar	44
10.1 Avvikelse och korrigerande åtgärd	44
10.2 Ständig förbättring	45
Bilaga A (informativ) Kontinuitetshantering vid höjd beredskap	46
Litteraturförteckning.....	56

Inledning

0.1 Bakgrund och syfte

0.1.1 Syfte och användningsområde

I detta dokument beskrivs nyttan med kontinuitetshantering baserat på den internationella standarden SS-EN ISO 22301. SS 22304 kompletterar SS-EN ISO 22313 men erbjuder mer praktisk vägledning om hur organisationer kan arbeta med kontinuitetshantering utifrån svenska förhållanden och med möjlig koppling till svenskt totalförsvaret. Denna sistnämnda koppling möjliggörs genom bilaga A som ger tilläggsrekommendationer för planering av kontinuitetshantering inför situationer med höjd beredskap då delar eller hela totalförsvaret mobiliseras. Bilaga A ger då stöd för de ändrade förutsättningar som uppstår vid ett regeringsbeslut om att gå upp i höjd beredskap.

SS 22304 kan fungera som praktisk handbok för hur kontinuitetshantering konkret kan planeras och läggas upp i en verksamhet. Detta dokument kan användas för att vara ett stöd för organisationer som har för avsikt att införa och tillämpa SS-EN ISO 22301 eller arbeta i enlighet med standardens intentioner.

I det här dokumentet beskrivs lämpliga steg som organisationen kan ta för att säkerställa att organisationen minimerar risker för allvarliga störningar samt att det finns förberedelser för att hantera allvarliga störningar när de inträffar.

0.1.2 Vad är kontinuitetshantering?

Kontinuitetshantering handlar om att systematiskt skapa en förmåga att fortsätta bedriva sin verksamhet med en acceptabel kapacitet. Detta gäller oberoende av vilken typ av störning som organisationen utsätts för. Vidare hanteras alla aspekter inom kontinuitet: från incident- till krishantering. Varje händelse och incident, stor eller liten, oavsett om den är oavsiktlig eller avsiktlig kan orsaka störningar i verksamheten. Kontinuitetshantering föreliggerenbart genom att det finns rätt förutsättningar och förberedelser inom organisationen.

Kontinuitetshantering handlar övergripande om att

- identifiera vilka delar av verksamheten som måste fungera för att undvika att organisationen drabbas av allvarliga konsekvenser vid en störning eller avbrott, dvs. att upprätthålla leveransen av varor eller tjänster på en acceptabel nivå,
- identifiera vilka kritiska resurser som krävs för att upprätthålla delar av verksamheten nödvändiga för att leverera viktiga varor eller tjänster, dvs. personer och roller, system, lokaler, infrastruktur och leverantörer,
- fastställa hur respektive kritisk resurskommer hanteras om den slås ut,
- genomföra de kontinuitetsstrategier som fastställts för att möta risker och bygga en krishanteringsförmåga,
- utforma, införa och dokumentera kontinuitetsplaner i verksamheten,
- testa fastställda kontinuitetslösningar samt utbilda och öva personal.

För att lyckas med kontinuitetshantering krävs allas engagemang och ett tydligt ledarskap samt att roller och ansvar är tydliga i organisationen.

0.1.3 Varför är kontinuitetshantering viktigt och vilka vinster finns det?

Genom kontinuitetshantering skapar organisationen bättre förutsättningar för att de viktigaste delarna av verksamheten upprätthålls även vid allvarligare störningar. Med kontinuitetshantering kan avbrottstiden reduceras och konsekvenserna begränsas vid en störning, se figur 1.

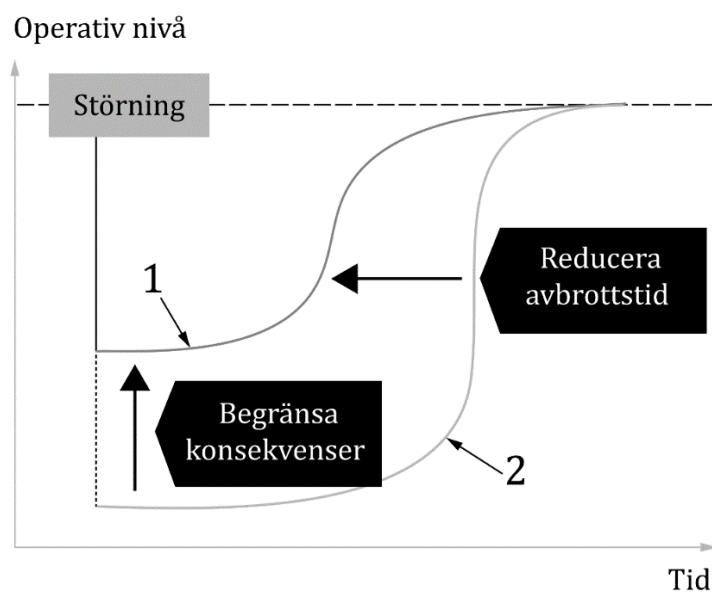
God kontinuitetshantering bidrar till ett mindre sårbart samhälle. Då samhället förändras och nya hot och risker utvecklas är det viktigt att företag och organisationer förbereder sig på att skapa en förmåga att hantera *olika sorters* störningar och avbrott i verksamheten så att dessa får en så liten påverkan som möjligt på verksamheten. Oftast går det inte att förutse alla *specifika* hot och risker. Därför är det viktigt att vara väl förberedd om det oförutsedda inträffar

SS 22304:2023 (sv)

Fördelarna med kontinuitet i verksamheten kan påvisas t.ex. genom att leveransen av varor och tjänster upprätthålls enligt en förutbestämd acceptabel nivå. Vinsterna blir att organisationen snabbare kan komma i gång vilket möjliggör kortare avbrottstider och genomförande av åtgärder, samt att det kan rädda mänskliga och stora ekonomiska värden som annars riskerar att gå förlorade. Detta under förutsättning att kontinuitetsplaneringen utförts på ett genomtänkt sätt.

Kontinuitetshantering innehåller ett förberedande arbete under vilket förutsättningar sätts för ett effektivt arbete i alla faser. Det är i det förebyggande arbetet som rutiner, planer, checklistor med mera utvecklas och införs i verksamheten genom utbildning, övning och testning. Dessa rutiner, planer och checklistor har olika syften och användningsområden, exempelvis används checklisten som en omedelbar åtgärd för att starta upp arbetet i verksamheten och direkt kunna mildra konsekvenserna av den inträffade händelsen.

Hur kontinuitetshanteringen förebygger och minskar verksamhetsförluster och avbrottstid (vid såväl plötsliga avbrott som vid gradvist utvecklade störningar) beskrivs schematiskt i figur 1.



Förklaring

1. Med kontinuitetshantering
2. Utan kontinuitetshantering

Figur 1 — Illustration av hur kontinuitetshanteringen förebygger och minskar verksamhetsförlust och avbrottstid

0.1.4 Vad är SS-EN ISO 22301?

SS-EN ISO 22301 är en internationell standard för styrning av en organisations kontinuitetshantering. standarden anges krav för att planera, upprätta, införa, tillämpa, övervaka, underhålla och ständigt förbättra ett dokumenterat ledningssystem för kontinuitetshantering. Genom att skapa en förmåga att förbereda inför, agera på och återställa verksamheten efter en störning eller ett avbrott kan organisationen upprätthålla leveransen av varor eller tjänster. Kraven i standarden är allmänna och avsedda att vara tillämpbara för varje organisation eller delar av en sådan, oavsett typ, storlek och inriktning. I vilken utsträckning kraven är tillämpbara är beroende av organisationens komplexitet och verksamhetsomgivning.

SS-EN ISO 22301 är tillämpbar för alla organisationer som vill

- upprätta, införa, underhålla och förbättra ett ledningssystem för kontinuitet,
- säkerställa att en fastställd kontinuitetspolicy följs,
- visa inför andra att organisationen arbetar efter standarden,
- söka certifiering av sitt ledningssystem från ett ackrediterat certifieringsorgan, eller
- göra en egen bedömning och egen förklaring av överensstämmelse med denna standard.

I likhet med andra ledningssystemstandards som SS-EN ISO 9001 för kvalitet, SS-EN ISO 14001 för miljö och SS-EN ISO/IEC 27001 för informationssäkerhet kan organisationer välja att certifiera sig mot SS-EN ISO 22301.

0.1.5 Hur hänger standarder inom ledningssystem för kontinuitetshantering ihop?

Följande standarder ingår i en serie där varje enskild standard har ett specifikt syfte men samtidigt kompletterar varandra:

- **SS-EN ISO 22300**, *Säkerhet och resiliens – Terminologi*, innehåller viktiga termer och definitioner inom området samhällssäkerhet och kan användas för att tolka den exakta innebörden av de krav och rekommendationer som specificeras i standarderna.
- **SS-EN ISO 22301**, *Säkerhet och resiliens – Ledningssystem för kontinuitetshantering – Krav*, innehåller kortfattade krav om vad organisationen förväntas uppfylla i sitt ledningssystem för kontinuitet.
- **SS 22304**, *Säkerhet och resiliens – Ledningssystem för kontinuitetshantering – Handbok för kontinuitetshantering enligt ISO 22301*, är en nationell standard som kompletterar ovanstående ISO-standarder med mer praktisk vägledning om hur organisationer arbetar med kontinuitetshantering.
- **SS-EN ISO 22313**, *Säkerhet och resiliens – Ledningssystem för kontinuitetshantering – Vägledning för implementering av ISO 22301*, ger kompletterande riktlinjer till hur en organisation uppfyller kraven i SS-EN ISO 22301.
- **SIS-ISO/TS 22317**, *Säkerhet och resiliens – Ledningssystem för kontinuitetshantering – Vägledning för konsekvensanalys*, innehåller rekommendationer för hur man gör en konsekvensanalys.
- **SIS-ISO/TS 22318**, *Säkerhet och resiliens – Ledningssystem för kontinuitetshantering – Vägledning för kontinuitet i försörjningskedjan*, innehåller rekommendationer för att utvidga principerna för verksamhetskontinuitet som ingår i SS-EN ISO 22301 och SS-EN ISO 22313 till hantering av leverantörsrelationer.
- **ISO/TS 22330**, *Säkerhet och resiliens – Ledningssystem för kontinuitet – "Guidelines for people aspects of business continuity"*, innehåller rekommendationer för planering och utveckling av policyer, strategier och procedurer för förberedelse och hantering av personer som drabbats av händelsen.
- **SIS-ISO/TS 22331**, *Säkerhet och resiliens – Ledningssystem för kontinuitet – Vägledning för att välja strategi för kontinuitet*, innehåller rekommendationer för urval och beslut av kontinuitetsstrategi.
- **SIS-ISO/TS 22332**, *Säkerhet och resiliens – Ledningssystem för kontinuitetshantering – Vägledning för att utforma kontinuitetsplaner och rutiner*, innehåller rekommendationer för att utveckla och underhålla effektiva kontinuitetsplaner och rutiner.

Standarder för ledningssystem som tas fram inom ISO utformas enligt ett enhetligt format. På så sätt säkerställs samstämmighet mellan SS-EN ISO 22301 och andra standarder för ledningssystem exempelvis SS-EN ISO 9001 om kvalitet, SS-EN ISO 14001 om miljö och SS-EN ISO/IEC 27001 om informationssäkerhet. Dessutom finns stöd för att ledningssystemet införs och tillämpas enhetligt och kan integreras med andra ledningssystem.

Vidare finns det andra ISO-standarder som kan vara relevanta i sammanhanget vid införande av SS-EN ISO 22301, exempelvis vägledningsstandarden SS-ISO 31000 som beskriver ett ramverk för riskhantering.

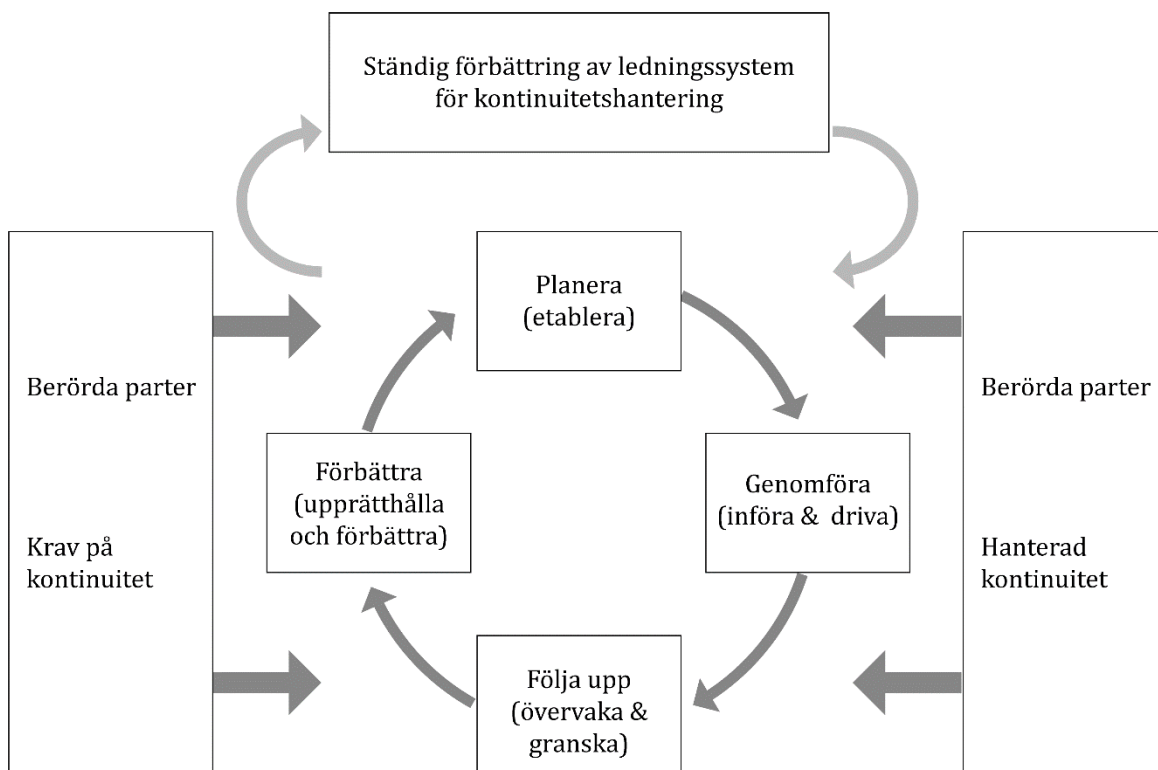
SS 22304:2023 (sv)

SS 22304 utgår från en svensk kontext och ger praktiska rekommendationer och exempel på hur kontinuitetshantering kan fungera i en verksamhet i såväl ett normalläge som inför och vid ett läge av höjd beredskap. Genom erfarenheter av hur god kontinuitetshantering upprätthålls i ett normalläge skapas också bättre förutsättningar för att även kunna upprätthålla god kontinuitetshantering i ett läge av höjd beredskap.

0.1.6 Plan-Do-Check-Act-modellen

PDCA-modellen (Plan-Do-Check-Act) kan tillämpas på alla processer och på ledningssystemet för kontinuitetshantering som helhet.

Hur PDCA-modellen kan användas för att Planera (etablera), Genomföra (införa och driva), Följa upp (övervaka och granska) och Förbättra (upprätthålla och förbättra), för att införa, upprätthålla och ständigt förbättra effektiviteten i en organisations ledningssystem för kontinuitetshantering beskrivs i figur 2 som är hämtad från SS-EN ISO 22313.



Figur 2 — PDCA-modellen tillämpad på processer för kontinuitetshantering

0.1.7 Läsanvisning

Detta dokument följer uppbyggnaden av den internationella standarden SS-EN ISO 22301. Varje avsnitt inleds med kravtexten från SS-EN ISO 22301 i en vit ruta följt av en vägledande text. Där så är relevant finns även exempel som används i dokumentets olika avsnitt.

För den som har för avsikt att implementera ett ledningssystem för kontinuitet och att certifiera organisationen rekommenderas att läsa och följa vägledningen i dokument.

För den som är intresserad av att få ett stöd i arbetet med kontinuitetshantering, men inte önskar gå så långt som till en certifiering, rekommenderas att i huvudsak fokusera på avsnitt 8 Verksamhet.

Om organisationen redan har ett etablerat ledningssystem i organisationen rekommenderas att, använda valda delar av denna vägledning för att komplettera med en kontinuitetsaspekt i det befintliga ledningssystemet. Särskilt viktiga är då avsnitten 5.3 Policy, 6 Planering och 8 Verksamhet.

De olika avsnitten i detta dokument innehåller följande:

Avsnitt 1 handlar om vägledningens omfattning och följs av avsnitt 2 med normativa hänvisningar och avsnitt 3 som är en lista med centrala termer och definitioner.

I avsnitt 4 beskrivs villkor som är nödvändiga för att bestämma förutsättningarna för organisationens ledningssystem för kontinuitet liksom behov, krav och omfattning.

Avsnitt 5 berör ledarskap och ledningens åtaganden. Ledningens engagemang är en avgörande förutsättning för framgångsrikt kontinuitetsarbete. Även policy, ansvar och befogenheter tas upp.

Avsnitt 6 handlar om planering för och mål med ledningssystemet. När åtgärder för att hantera risker och möjligheter genomförs bör verksamheten utgå från det som har beskrivits i avsnitt 4 och avsnitt 5 gällande verksamheten, dess syfte och mål. Det är genom dessa aktiviteter som ledningssystemets risker identifieras.

Avsnitt 7 handlar om det stöd som behöver finnas både för ledningssystemet och för att upprätthålla kontinuitetsarbetet. Det gäller såväl resurser, kompetens, medvetenhet, kommunikation som dokumenterad information.

Avsnitt 8 beskriver hur kontinuitetshantering bör genomföras i organisationen. Eftersom detta avsnitt är mycket omfattande, ger vi här en mer detaljerad läsanvisning för varje delavsnitt.

8.1 Planering och styrning av verksamheten innefattar processer för att styra verksamheten så att de planerade åtgärder, som beskrivs i 6.1 Åtgärder för att hantera risker och möjligheter, kan genomföras. Detta inkluderar inventering av vad organisationen redan har upprättat i form av verksamhetsplanering, processbeskrivningar, planer, rutiner, system och användarkrav, behovsanalys med mera.

8.2 Konsekvensanalys och riskbedömning beskriver hur konsekvensanalys och riskbedömning bör genomföras i organisationen. En konsekvensanalys lägger grunden till att kartlägga vilka aktiviteter som är prioriterade och måste upprätthållas samt vilka resurser som är nödvändiga för att genomföra dessa aktiviteter. Riskbedömningen bidrar till en förståelse för de risker som kan leda till avbrott i verksamheten.

8.3 Kontinuitetsstrategier och lösningar beskriver hur kontinuitetsstrategier och lösningar bör upprättas för organisationen vilket inkluderar olika alternativ för att hantera en störning såväl före, under och efter att den inträffat.

8.4 Kontinuitetsplaner och rutiner beskriver hur organisationen bör utveckla och förvalta kontinuitetsplaner som svarar mot organisationens behov. Målet är en samling relevanta, aktuella och dokumenterade kontinuitetsplaner som är tillgängliga för berörda personer och grupper.

8.5 Övningsprogram beskriver hur organisationen bör genomföra övning och testning. Övning och testning är grundläggande för att utveckla organisationens förmåga att hantera avbrott och störningar i verksamheten. Övningar och tester ger organisationen möjlighet att validera fastställda strategier och lösningar.

8.6 Utvärdering av dokumentation och kontinuitetsförmågor beskriver hur systematisk utvärdering kan genomföras av organisationens kontinuitetshantering.

Avsnitt 9 beskriver hur organisationen bör utvärdera och övervaka ledningssystemets prestanda. Detta är centralt för att skapa förutsättningar för att ständigt förbättra kontinuitetsförmågan i organisationen.

I avsnitt 10 ges ingen kompletterande vägledning då kraven anses vara självförklarande.

Vid krig eller fara för krig kan regeringen besluta om höjd beredskap i hela eller delar av Sverige.

SS 22304:2023 (sv)

I bilaga A Kontinuitetshantering inför höjd beredskap ges vägledning för att kunna tillämpa ledningssystem för kontinuitet både inför och under höjd beredskap. Denna bilaga beskriver de ändrade förutsättningar som gäller vid höjd beredskap och vad organisationen bör tänka på.

0.2 Koppling till standardisering inom CEN och ISO

Detta dokument är relaterat till andra dokument framtagna av ISO/TC 292 *Security and resilience*. Denna ISO-kommitté har tagit fram en familj av internationella standarder och tekniska specifikationer vilket redogörs för i 0.1.5.

Två av dokumenten i omnämnda familj, SS-EN ISO 22301 och SS-EN ISO 22313, är båda fastställda som europeiska standarder av CEN/TC 391 *Societal and Citizen Security*. I SS-EN ISO 22313 ges en generell vägledning om kraven i SS-EN ISO 22301 men alla aspekter av kontinuitetshanteringen täcks inte in.

Innehållet i SS 22304 kompletterar dessa två standarder med mer praktisk vägledning och stöd för hur man kan arbeta konkret med kontinuitetshantering utifrån svenska förhållanden och med möjlig koppling till svenskt totalförsvaret. Således är detta dokument inte i konflikt med CEN:s frysningsregel.

0.3 Koppling till lagstiftning

Detta dokument är inte direkt kopplat till lagstiftning men kontinuitetshantering som metodik rekommenderas i MSB:s metodstöd för skydd av samhällsviktig verksamhet. Detta dokument nämner ett antal lagar och föreskrifter inom området totalförsvaret.

0.4 Väsentliga skillnader mot föregående utgåva

De huvudsakliga förändringarna i förhållande till den föregående utgåvan är:

- Texter har uppdaterats i enlighet med nya utgåvan av SS-EN ISO 22301.
- Det är säkerställt att standarden inte är motstridig med SS-EN ISO 22313 samt kompletterar dess innehåll.
- Den vägledande texten har i stor omfattning förtydligats och anpassats till krav ställda i SS-EN ISO 22301 ställda krav. Detta gäller särskilt avsnitt 8.
- Bilaga A har lagts till där vägledning erhålls kring hur kontinuitetshantering bör bedrivas inför och under höjd beredskap.

1 Omfattning

I detta dokument ges praktiska rekommendationer om konkret kontinuitetshantering samt verktyg, exempel och mallar som utgår från svenska förhållanden för hur man kan gå till väga.

I detta dokument finns även en bilaga med tilläggsrekommendationer för kontinuitetshantering inför och vid höjd beredskap.

Anmärkning: Detta dokument utgår från och kompletterar vägledningen i SS-EN ISO 22313. Dessutom innehåller detta dokument samtliga krav från SS-EN ISO 22301.

Detta dokument kan tillämpas av alla typer av organisationer i Sverige, oavsett typ, storlek och inriktning när de behöver skapa en förmåga att hantera avbrott eller störningar i verksamheten, dvs. ha kontinuitet i sin verksamhet. Detta dokument kan tillämpas av den eller de som fått i uppdrag att leda, implementera eller förvalta kontinuitetshantering i organisationen.

2 Normativa hänvisningar

Detta dokument innehåller inte några normativa hänvisningar.

Anmärkning 1: En förutsättning för att använda det här dokumentet är att följa kraven i SS-EN ISO 22301 men eftersom de återfinns i sin helhet kopierade i detta dokument är det inte nödvändigt att använda SS-EN ISO 22301 parallellt med detta dokument.

Anmärkning 2: SS-EN ISO 22301 hänvisar normativt endast till ISO 22300, för terminologin.

3 Termer och definitioner

I detta dokument gäller följande termer och definitioner.

3.1

kontinuitet

en organisations strategiska och taktiska förmåga, som i förväg är godkänd av ledningen, för att planera för och agera på förhållanden, situationer och händelser i syfte att upprätthålla verksamheten på en acceptabel förutbestämd nivå

Anmärkning 1 till termpost: Kontinuitet är den mer generella termen för operationell kontinuitet och verksamhetskontinuitet som säkerställer att en organisation kan fortsätta med sin verksamhet även utanför normala driftsförhållanden. Detta tillämpas inte enbart på vinstdrivande företag, utan på alla typer av organisationer, t.ex. statliga och icke-statliga organisationer och organisationer av allmänintresse.

[Källa: SS-EN ISO 22300:2021, 3.1.50, översatt]

3.2

verksamhetskontinuitet

förmåga hos en organisation att fortsätta tillhandahålla *produkter och tjänster* (3.15) inom acceptabla tidsramar enligt en förutbestämd kapacitet vid en *störning* (3.6)

[Källa: SS-EN ISO 22300:2021, 3.1.19, översatt]

3.3

kontinuitetshantering

process för att implementera och underhålla *verksamhetskontinuitet* (3.2)

[Källa: SS-EN ISO 22300:2021, 3.1.20, översatt]

SS 22304:2023 (sv)

3.4

kontinuitetsplan

dokumenterad information som vägleder en organisation att hantera en *störning* (3.6) och återuppta, återställa och återupprätta leveransen av *produkter och tjänster* (3.15) i överensstämmelse med dess mål för *kontinuitetshantering* (3.3)

[Källa: SS-EN ISO 22300:2021, 3.1.22, översatt]

3.5

konsekvensanalys

process för analys av *konsekvens* (3.11) på verksamhet som en *störning* (3.6) över tid får på organisationen

Anmärkning 1 till termpost: Utfallet av konsekvensanalysen är en förklaring och motivering av krav för verksamhetskontinuitet.

[Källa: SS-EN ISO 22300:2021, 3.1.24, översatt]

3.6

störning

incident (3.12), som kan vara förutsedd eller oförutsedd, som orsakar en oplanerad, negativ avvikelse från den förväntade leveransen av *produkter och tjänster* (3.15) i enlighet med en organisations mål

Anmärkning 1 till termpost: I detta dokument används båda termerna störning och avbrott. Störning är ett vidare begrepp som kan inkludera begreppet avbrott. Störning fokuserar på leveransen av produkten eller tjänsten.

[Källa: SS-EN ISO 22300:2021, 3.1.75, översatt – anmärkning 1 till termpost har lagts till]

3.7

avbrott

incident (3.12) som leder till icke-förväntat upphörande av *aktivitet* (3.13)

Anmärkning 1 till termpost: I detta dokument används båda termerna störning och avbrott. Avbrott är ett snävare begrepp än störning. Avbrott fokuserar på genomförandet av organisationens prioriterade aktiviteter.

3.8

maximal tolerabel avbrottstid

MTA

tid det tar innan det uppstår en oacceptabel negativ påverkan, till följd av att en *produkt eller tjänst* (3.15) inte tillhandahålls eller att en *aktivitet* (3.13) inte utförs

en maximum tolerable period of disruption, MTPD
maximum acceptable outage, MAO

[Källa: SS-EN ISO 22300:2021, 3.1.151, översatt]

3.9

mål för återställningstid

RTO

tid det tar innan en *produkt och tjänst* (3.15) eller en *aktivitet* (3.13) återupptas eller resurser återställs efter en *incident* (3.12)

Anmärkning 1 till termpost: För produkter, tjänster och aktiviteter understiger RTO den tid det skulle ta innan den negativa påverkan blir oacceptabel på grund av att en produkt eller tjänst inte tillhandahålls eller en aktivitet inte utförs.

en recovery time objective

[Källa: SS-EN ISO 22300:2021, 3.1.203, översatt]

3.10

mål för återställningspunkt

RPO

punkt till vilken informationen som används av en *aktivitet* (3.13) återställs för att kunna återuppta aktiviteten

Anmärkning 1 till termpost: Kan även refereras till som "maximal dataförlust".

en recovery point objective

[Källa: SS-EN ISO 22300:2021, 3.1.202, översatt]

3.11

konsekvens

utfall av en händelse som påverkar mål

Anmärkning 1 till termpost: En konsekvens kan vara känd eller okänd och kan ha positiva eller negativa, direkta eller indirekta, effekter på målen.

Anmärkning 2 till termpost: Konsekvenser kan uttryckas kvalitativt eller kvantitativt.

Anmärkning 3 till termpost: Konsekvenser kan eskalera genom kaskadeffekter och kumulativa effekter.

[Källa: SS-EN ISO 22300:2021, 3.1.45, översatt]

3.12

incident

händelse som kan vara eller skulle kunna leda till en *störning* (3.6), en förlust, ett nödläge eller en kris

[Källa: SS-EN ISO 22300:2021, 3.1.122, översatt]

3.13

aktivitet

uppsättning av en eller flera uppgifter med ett definierat utfall

[Källa: SS-EN ISO 22300:2021, 3.1.2, översatt]

3.14

prioriterad aktivitet

aktivitet (3.13) som tilldelas hög angelägenhetsgrad för att undvika oacceptabel påverkan på verksamheten vid en *störning* (3.6)

[Källa: SS-EN ISO 22300:2021, 3.1.186, översatt]

3.15

produkt och tjänst

utfall eller resultat som tillhandahålls av en organisation till berörda parter

Exempel: Tillverkade varor, bilförsäkring, sjukskötersketjänster

[Källa: SS-EN ISO 22300:2021, 3.1.191, översatt]

3.16

resurs

alla tillgångar (inklusive anläggning och utrustning), människor, färdigheter, teknik, lokaler samt varor och information (elektronisk eller annan) som en organisation måste ha tillgängliga att utnyttja när de behövs, för att bedriva verksamheten och nå sitt mål

[Källa: SS-EN ISO 22300:2021, 3.1.207, översatt]

3.17

risk

osäkerhetens effekt på mål

Anmärkning 1 till termpost: En effekt är en avvikelse från det förväntade. Den kan vara positiv eller negativ samt kan avse, ge upphov till eller resultera i möjligheter och hot.

SS 22304:2023 (sv)

Anmärkning 2 till termpost: Mål kan ha olika aspekter, ingå i olika kategorier och gälla på olika nivåer.

Anmärkning 3 till termpost: Risker uttrycks vanligtvis som riskkällor, potentiella händelser, deras konsekvenser och deras sannolikhet.

Anmärkning 4 till termpost: Detta är en av de allmänna termerna och en av de viktigaste definitionerna i högnivåstrukturen för ISO-ledningssystemstandarder. Termposten har hämtats från ISO 31000:2018, 3.1, där orden "på mål" har lagts till i definitionen anmärkningarna till termposten har ersatts.]

[Källa: SS-EN ISO 22300:2021, 3.1.215, översatt]

3.18

riskbedömning

övergripande process för riskidentifiering, riskanalys och riskutvärdering

Anmärkning 1 till termpost: Riskbedömning innehåller processen att identifiera interna och externa hot och sårbarheter, identifiera sannolikhet för och påverkan av att en händelse uppstår på grund av sådana hot eller sårbarheter, definiera kritiska funktioner som krävs för kontinuitet av organisationens verksamhet, definiera kontrollerna som krävs för att reducera utsattheten samt utvärdera kostnaderna för sådana kontroller.

Anmärkning 2 till termpost: Riskbedömning beskrivs ingående i ISO 31000:2018.

[Källa: SS-EN ISO 22300:2021, 3.1.219, översatt]

3.19

försörjningskedja

tvåvägsrelation mellan organisationer, personer, processer, logistik, information, teknik och *resurser* (3.16) som ingår i *aktiviteterna* (3.13) och skapar värde hela vägen från inköp av material till leverans av *produkter eller tjänster* (3.15)

Anm.1 till termpost: Försörjningskedjan kan inkludera leverantörer av olika slag så som säljare, underentreprenörer, faciliteter för tillverkning, logistikleverantörer, interna distributionscenter, distributörer, grossister och andra enheter som leder till slutanvändaren.

[Källa: SS-EN ISO 22300:2021, 3.1.271, översatt]

4 Organisationens förutsättningar

4.1 Att förstå organisationen och dess förutsättningar

Mål: Att skapa en gemensam förståelse för organisationens verksamhet.

Resultat: En dokumenterad verksamhetsbeskrivning.

Krav från SS-EN ISO 22301:

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 kontinuitetshantering.

Anmärkning: De identifierade relevanta frågorna kommer att påverkas av organisationens övergripande mål, dess produkter och tjänster och graden och typen av risk som organisationen kan komma att ta.

När verksamheten avgör vilka externa och interna frågor som är relevanta bör följande frågor beaktas:

- Vilka är våra styrkor, svagheter och vilka hot och möjligheter kan vi identifiera? (*SWOT*-analys)
- Vilken är vår kärnverksamhet och branschtillhörighet?
- Vilken kompetens har vi?
- Vilka unika kunskaper finns i organisationen?
- Vilka personella, tekniska och finansiella resurser finns tillgängliga?
- Hur ser vår försörjningskedja ut?
- Vilka relationer har vi till kunder, leverantörer och övriga intressenter?

- Hur gör våra konkurrenter och hur gör man i andra branscher?

4.2 Att förstå berörda parter behov och förväntningar

4.2.1 Allmänt

Mål: Att förstå berörda parter.

Resultat: Berörda parter och deras krav är identifierade.

Krav från SS-EN ISO 22301:

När organisationen fastställer sitt ledningssystem för kontinuitetshantering ska den bestämma

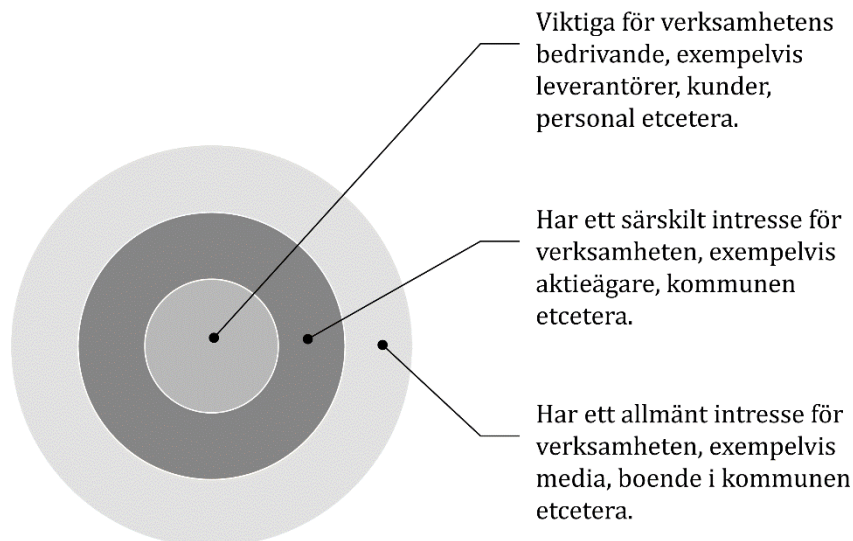
- vilka berörda parter som är relevanta för ledningssystemet för kontinuitetshantering,
- vilka av dessa berörda parter krav som är relevanta.

För att bedöma vilka de berörda parterna är så bör man främst utgå från målgruppen för organisationens produkter och/eller tjänster.

Exempel på berörda parter är anställda, kunder eller brukare, leverantörer, partner och myndigheter.

Relevanta krav kan bland annat vara avtalskrav i upphandlingar av organisationens varor eller tjänster men kan också handla om outtalade förväntningar, t.ex. avseende leveranstid för en viss produkt eller tjänst. Vidare kan olika målgrupper ha olika förväntningar på samma produkt eller tjänst.

När berörda parter analyseras bör de grupperas utifrån deras betydelse för organisationen. Detta beskrivs i figur 3 som kan vara till hjälp för att prioritera mellan krav från olika berörda parter.



Figur 3 — Hur berörda parter kan analyseras utifrån deras betydelse för verksamheten

SS 22304:2023 (sv)

4.2.2 Författningskrav

Mål: Att ta hänsyn till och uppfylla aktuella och relevanta författningskrav och andra krav.

Resultat: Relevanta författningskrav, t.ex. lagar och förordningar och andra krav, är identifierade och dokumenterade.

Krav från SS-EN ISO 22301:

Organisationen ska

- a) införa och vidmakthålla en process för att identifiera, ha tillgång till och bedöma de tillämpliga rättsliga och regelmässiga krav som är relaterade till kontinuiteten för dess produkter och tjänster, aktiviteter och resurser,
- b) säkerställa att dessa tillämpliga rättsliga, regelmässiga och andra krav beaktas vid införandet och vidmakthållandet av dess ledningssystem för kontinuitetshantering,
- c) dokumentera denna information och hålla den aktuell.

När man identifierar relevanta krav bör organisationen ta särskild hänsyn till författningskrav gällande myndighetstillstånd.

4.3 Att bestämma ledningssystemets omfattning

Mål: Att definiera ledningssystemets omfattning.

Resultat: Ledningssystemets omfattning är definierad och fastställd.

4.3.1 Allmänt

Krav från SS-EN ISO 22301:

Organisationen ska bestämma avgränsningar och tillämpligheten av ledningssystemet för kontinuitetshantering för att fastställa dess omfattning.

När organisationen bestämmer denna omfattning ska den beakta

- a) de externa och interna frågor som det hänvisas till i 4.1,
- b) de krav från berörda parter som det hänvisas till i 4.2,
- c) dess uppdrag, mål och interna och externa åtaganden.

Omfattningen ska finnas tillgänglig som dokumenterad information.

Här ges ingen kompletterande vägledning då kraven anses vara självförklarande.

4.3.2 Ledningssystemets omfattning

Krav från SS-EN ISO 22301:

Organisationen ska

- a) fastställa de delar av organisationen som ska inkluderas i ledningssystemet för kontinuitetshantering, med beaktande av dess plats(er), storlek, beskaffenhet och komplexitet,
- b) identifiera produkter och tjänster som ska inkluderas i ledningssystemet för kontinuitetshantering.

När omfattningen definieras ska organisationen dokumentera och förklara uteslutanden. Alla sådana uteslutanden ska förklaras och ska inte påverka organisationens förmåga och ansvar för att tillhandahålla kontinuitetshantering, enligt vad som anges i konsekvensanalysen eller riskbedömningen och tillämpliga rättsliga eller regelmässiga krav.

För att kunna fastställa vilka delar av organisationen som omfattas bör följande aspekter beaktas:

- Organisationens övergripande vision och mål och, i synnerhet, de produkter och tjänster som är centrala för organisationens syfte.
- Vilka organisationens viktigaste produkter och tjänster är, t.ex. utifrån volym, omsättning, vinstmarginal, målgrupp med mera.
- Vilka risker som påverkar organisationen.
- Författningskrav.

Tänk på att alla delar inom organisationen inte behöver ingå när ledningssystemets omfattning definieras.

4.4 Ledningssystem för kontinuitetshantering

Krav från SS-EN ISO 22301:

Organisationen ska upprätta, tillämpa, upprätthålla och ständigt förbättra ett ledningssystem för kontinuitetshantering, inklusive nödvändiga processer och deras samverkan, enligt kraven i detta dokument.

Anmärkning: ISO:s standarder för ledningssystem tillämpar en gemensam harmoniserad struktur för att underlätta för en organisation att implementera flera ledningssystemstandarder som då kan integreras med varandra. Om organisationen redan har implementerat ledningssystem i enlighet med en annan ISO-standard (t.ex. SS-EN ISO 9001 eller SS-EN ISO 14001) är det lämpligt att detta används som grund när man för in kraven från SS-EN ISO 22301.

Här ges ingen kompletterande vägledning då kraven anses vara självförklarande.

5 Ledarskap

5.1 Ledarskap och åtagande

Mål: Att ledarskapet gällande ledningssystemet för kontinuitetshantering är tydligt och kommunicerat.

Resultat: Ett tydligt ledarskap gällande ledningssystemet för kontinuitetshantering är dokumenterat och kommunicerat i organisationen.

Krav från SS-EN ISO 22301:

Högsta ledningen ska tydligt visa ledarskap och engagemang i fråga om ledningssystemet för kontinuitetshantering genom att

- a) säkerställa att kontinuitetspolicy och kontinuitetsmål är upprättade för ledningssystemet och är förenliga med organisationens förutsättningar och strategiska inriktning,
- b) säkerställa att kraven i ledningssystemet integreras i organisationens verksamhetsprocesser,
- c) säkerställa att ledningssystemet ges nödvändiga resurser,
- d) kommunicera betydelsen av att ledningssystemet leds och styrs på ett väl fungerande sätt och att kraven i ledningssystemet uppfylls,
- e) säkerställa att ledningssystemet för kontinuitetshantering uppnår avsett resultat,
- f) leda och stödja personer så att de bidrar till ett väl fungerande ledningssystem,
- g) främja ständig förbättring,
- h) ge stöd till andra relevanta ledande befattningshavare så att de tydligt utövar sitt ledarskap på ett sätt som är lämpligt inom deras ansvarsområden.

Anmärkning Hänvisningar till "verksamhet" i detta dokument kan ges en bred tolkning, nämligen de aktiviteter som är centrala för syftet med organisationens existens.

SS 22304:2023 (sv)

Det är alltid ledningen som har det yttersta ansvaret för kontinuitetshanteringen i organisationen. Ledningens uppgift är att verka för att kontinuitetsarbetet i organisationen ges förutsättningar för att vara en integrerad och kontinuerlig process i ordinarie verksamhet och att skapa en medvetenhet om och förståelse för kontinuitetshanteringen.

Kontinuitetshantering handlar om att upprätthålla en effektiv affärs- och verksamhetsstyrning även under störning i verksamheten. Därför är ledningens åtagande en avgörande förutsättning för framgångsrikt kontinuitetsarbete.

När kontinuitetsarbetet genomförs bör ledningen kontinuerligt följa arbetet. Den person eller funktion som fått ansvar för att samordna och driva kontinuitetsarbetet bör ges möjlighet att löpande redovisa för ledningen hur arbetet fortskrider. Ledningen bör också aktivt stödja arbetet med kontinuitetshantering genom att föra upp frågan på dagordningen i organisationens olika verksamhetsdelar. Det är även ledningens ansvar att säkerställa att det finns tillräckliga resurser och befogenheter för att kunna utföra kontinuitetsarbetet enligt ledningens ambitioner och riktlinjer. Beslut som fattas av ledningen under planering och implementering av kontinuitetsarbete bör spridas i organisationen i syfte att förankra ledningens intentioner.

5.2 Policy

5.2.1 Upprättande av kontinuitetspolicy

Mål: Att skapa en kontinuitetspolicy som sätter ramverket för arbetet med kontinuitetshantering.

Resultat: En kontinuitetspolicy, som är anpassad till organisationens förutsättningar, är dokumenterad, fastställd och kommunicerad till relevanta berörda parter.

Krav från SS-EN ISO 22301:

Högsta ledningen ska upprätta en policy för kontinuitetshantering som

- a) är anpassad till organisationens syfte,
- b) ger ett ramverk för att sätta kontinuitetsmål,
- c) innefattar ett åtagande att uppfylla tillämpliga krav,
- d) innefattar ett åtagande att ständigt förbättra ledningssystemet för kontinuitetshantering.

Syftet med en kontinuitetspolicy är att, till berörda parter, kommunicera vilka principer organisationen tillämpar, se 5.2.2.

En kontinuitetspolicy bör visa ledningens övergripande mål och förväntningar samt dess syn på organisationens kontinuitetshantering. En kontinuitetspolicy bör vara kortfattad, lättläst, tydlig och bör kompletteras med riktlinjer och rutiner för att ge organisationen en dokumenterad styrning av sitt kontinuitetsarbete.

Kontinuitetspolicyen tillhandahåller principer som organisationen strävar efter att uppfylla och använda som måttstock för att kunna uppnå målsättningarna. Dess innehåll består bland annat av lagstadgade, reglerande och avtalsenliga förpliktelser samt organisationens huvudsakliga berörda parter. Kontinuitetspolicyen bör vara väl förankrad utifrån organisationens förutsättningar, se avsnitt 4.

Kontinuitetspolicyen bör definiera ambitionsnivå, befogenheter och ansvarsfördelning inom kontinuitetsområdet. Den bör också fastställa organisatoriska mål och ledningsmål som ligger till grund för att fastställa relevanta aktiviteter och åtgärder för att minska risker.

En kontinuitetspolicy kan innehålla en beskrivning av nyckelpersoner och deras ansvar, tydliggöra förväntningar på ansvariga, ledningen och övrig berörd personal.

Kontinuitetspolicyen bör regelbundet utvärderas utifrån organisationens mål samt erfarenheter från kontinuitetsarbetet och bör vid behov revideras.

5.2.2 Kommunikation av kontinuitetspolicy

Krav från SS-EN ISO 22301:

Polycyn ska

- a) finnas tillgänglig som dokumenterad information,
- b) kommuniceras inom organisationen,
- c) i tillämplig utsträckning finnas tillgänglig för berörda parter.

Organisationens kontinuitetspolicyer bör kommuniceras till alla berörda parter så att de är införstådda med vilka principer som styr arbetet med kontinuitetshantering. Detta sker i första hand genom att kommunicera kontinuitetspolycyn på samma sätt som organisationens övriga policys, t.ex. via ett intranät samt extern hemsida.

Vidare kan polycyn kommuniceras direkt till utvalda berörda parter genom riktade informationsinsatser som exempelvis nyhetsbrev, både interna och externa.

Riktade informationsinsatser bör särskilt genomföras vid ändringar i polycyn. Oftast är det en kombination av kommunikationsåtgärder som ger bäst effekt.

5.3 Roller, ansvar och befogenheter

Mål: Att ansvar och befogenheter är tydligt beskrivna i organisationen.

Resultat: Ansvar och befogenheter är kommunicerade i organisationen.

Krav från SS-EN ISO 22301:

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 kontinuitetshantering överensstämmer med kraven i detta dokument,
- b) rapportera till högsta ledningen hur ledningssystemet för kontinuitetshantering fungerar.

Det är högsta ledningen som skapar rätt förutsättningar och tilldelar ansvar för kontinuitetshantering. Ansvaret bör tydliggöras i en rollbeskrivning.

För att skapa rätt förutsättningar bör högsta ledningen säkerställa att

- tillräckliga resurser finns,
- ansvar och befogenheter för relevanta roller har dokumenterats och kommunicerats till berörda parter, och
- kontinuitetshanteringen implementeras.

Beroende på storlek på organisationen och verksamhetens beskaffenhet kan ansvaret för ledningssystemet fördelas på olika roller. Ansvaret kan antingen ligga i kärnverksamheten eller i en stödjande del av organisationen.

Exempel på relevanta befattningar är

- produktionschef,
- verksamhetschef,
- kontinuitetsansvarig,
- riskhanteringsansvarig,
- säkerhetschef,
- beredskapschef.

SS 22304:2023 (sv)

Representanter från olika delar i verksamheten bör utses att vara stödjande i genomförandet av kontinuitetsarbetet.

Exempel på relevanta roller är

- beredskapssamordnare,
- säkerhetssamordnare,
- säkerhetsstrateg.

6 Planering

6.1 Åtgärder för att hantera risker och möjligheter

Mål: Att identifiera och hantera de risker och möjligheter som påverkar ledningssystemet för kontinuitetshantering.

Resultat: En dokumenterad riskbedömning som beskriver risker och möjligheter samt åtgärder för att hantera dessa så att ledningssystemet ger avsett resultat.

6.1.1 Fastställa risker och möjligheter

Krav från SS-EN ISO 22301:

När organisationen planerar ledningssystemet för kontinuitetshantering ska den beakta de frågor som det 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) försäkra sig om att ledningssystemet har möjlighet att ge avsett resultat,
- b) förebygga eller minska oönskade konsekvenser,
- c) uppnå ständig förbättring.

I SS-EN ISO 22301 finns två avsnitt som berör risk:

- 6.1.1 handlar om att fastställa risker och möjligheter gällande ledningssystemets effektivitet.
- 8.2.3 fokuserar på att göra en riskbedömning av störning i verksamhetens prioriterade aktiviteter och nödvändiga resurser.

När risker och möjligheter gällande ledningssystemets effektivitet identifieras bör organisationen beakta de aspekter som kan komma att påverka ledningssystemets resultat. Risker i detta sammanhang är de osäkerheter som gör att målet inte kan nås med ledningssystemet och dess verksamhet.

Exempel på risker och möjligheter för ledningssystemet är

- otydligt mandat från ledningen,
- otillräckliga resurser,
- bristfällig eller otillgänglig information,
- oengagerad personal eller personal med bristfällig kompetens,
- förändringar i interna och externa krav,
- omvärldsläge.

Med avsett resultat i detta fall menas ett ledningssystem som möjliggör ett fungerande och systematiskt kontinuitetshanteringsarbete inom organisationen.

Oönskade konsekvenser kan t.ex. vara att ledningssystemet

- inte leder till suboptimering och styr verksamheten i fel riktning,
- inte implementeras ordentligt,
- inte integreras i organisationens befintliga ledningssystem.

Risker och möjligheter bör löpande ses över exempelvis vid organisationsförändringar.

Inom organisationen kan det finnas genomförda riskanalyser som ger ett bra underlag för identifiering av risker och möjligheter utifrån organisationens kontext.

6.1.2 Hantering av risker och möjligheter

Krav från SS-EN ISO 22301:

Organisationen ska planera

a) åtgärder för att hantera dessa risker och möjligheter,

b) hur den ska

1) integrera och införa åtgärderna i processerna inom sitt ledningssystem, se 8.1,

2) utvärdera om åtgärderna har gett avsedd verkan, se 9.1.

Anmärkning: Risker och möjligheter avser ledningssystemets ändamålsenlighet. Risker som har relation till störning i verksamheten behandlas i 8.2.

Här ges ingen vägledning då kraven är beroende av det som har identifierats i föregående avsnitt där även exempel ges.

6.2 Kontinuitetsmål och planering för att uppnå dem

Mål: Att definiera och uppnå verksamhetens kontinuitetsmål.

Resultat: Dokumenterade och fastställda kontinuitetsmål, samt en plan för hur dessa mål uppnås, tas fram och följs upp kontinuerligt.

6.2.1 Upprätta kontinuitetsmål

Krav från SS-EN ISO 22301:

Organisationen ska upprätta kontinuitetsmål för relevanta funktioner och nivåer.

Kontinuitetsmålen för verksamheten ska

a) stå i överensstämmelse med kontinuitetspolicyn

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

c) ta hänsyn till tillämpliga krav, se 4.1 och 4.2,

d) övervakas,

e) kommuniceras,

f) uppdateras efter behov.

Organisationen ska bevara dokumenterad information om kontinuitetsmålen.

Med ett kontinuitetsmål menas ett mål som beskriver vad verksamheten klarar av under vissa omständigheter. Det kan t.ex. röra sig om mål kopplade till leverans, resultat, drift eller ekonomi. Målen kan bland annat röra leveranskrav till kund, eller driftkrav som ställs av kund. Oavsett karaktär handlar det om aktuella prestationsmål och krav där leveransförmågan är i fokus, vare sig vi talar om varor eller tjänster.

SS 22304:2023 (sv)

Exempel på kontinuitetsmål:

- Organisationen kan, vid avbrott, möta 80 % av kunders beställningar i enlighet med gällande avtal.
- Organisationen kan alltid leverera prioriterade varor och tjänster till våra viktigaste kunder.
- Ett avbrott i prioriterade varor och tjänster leder inte till mer än 5 % av förlorade marknadsandelar.

Kontinuitetsmål kan tas fram för olika delar av eller nivåer inom organisationen, t.ex. för olika verksamheter. Olika produkter och tjänster kan ha olika kontinuitetsmål.

6.2.2 Fastställa kontinuitetsmål

Krav från SS-EN ISO 22301:

När organisationen planerar för att uppnå sina kontinuitetsmål ska den fastställa

- a) vad som ska göras,
- b) vilka resurser som kommer att krävas,
- c) vem som ska vara ansvarig,
- d) när det ska vara genomfört,
- e) hur resultaten ska utvärderas.

Efter att målen är upprättade planerar organisationen för hur den uppnår dessa mål.

Som stöd för arbetet kan informationen samlas i någon form av plan, se tabell 1.

Tabell 1 – Exempel på innehåll i plan för fastställande av kontinuitetsmål

	Förklarande text
Mål	Beskrivning av kontinuitetsmål.
Resurser	Beskrivning av vilka resurser som behövs för att nå uppsatta mål. Vanliga resurser är personal, nyckelkompetens, ekonomi, investeringar, lokaler med mera.
Ansvarig	Beskrivning av vem som är ansvarig, t.ex. en enskild verksamhet, chef, ledning med mera.
Tidplan	Beskrivning av när i tid olika delar av arbetet med kontinuitetshantering förväntas vara färdiga.
Utvärdering	Beskrivning av hur resultatet ska utvärderas, t.ex. genom en enskild process eller som en integrerad del i befintliga processer inom organisationen.

6.3 Planering av förändring

Mål: Att skapa förutsättningar för att hantera behov av förändringar av ledningssystemet

Resultat: Behov av förändringar av ledningssystemet finns fastställda.

Krav från SS-EN ISO 22301:

När organisationen fastställer behovet av ändringar av ledningssystemet för kontinuitetshantering, inklusive de som definieras i avsnitt 10, ska ändringarna göras på ett planerat sätt.

Organisationen ska överväga

- a) syftet med ändringarna och deras möjliga konsekvenser,
- b) riktigheten hos ledningssystemet för kontinuitetshantering,

- c) tillgången till resurser,
d) fördelning eller omfördelning av ansvar och befogenheter.

Här ges ingen kompletterande vägledning då kraven anses vara självförklarande.

7 Stöd

7.1 Resurser

Mål: Att fastställa nödvändiga resurser för att upprätta, införa, underhålla och ständigt förbättra ledningssystemet för kontinuitet.

Resultat: Nödvändiga resurser tillhandahålls.

Krav från SS-EN ISO 22301:

Organisationen ska fastställa och tillhandahålla de resurser som behövs för att upprätta, införa, underhålla och ständigt förbättra ledningssystemet för kontinuitetshantering.

Anmärkning: Detta avsnitt rör ledningssystemet, inte kontinuitetslösningarna som beskrivs i 8.3.4.

För att fastställa vilka resurser som behövs bör organisationen analysera vilka behov ledningssystemet har. Detta inkluderar t.ex. personal, kompetens och programvaror.

7.2 Kompetens

Mål: Att säkerställa kompetensen hos berörd personal.

Resultat: Personalen är lämpad och kompetent nog för sina arbetsuppgifter.

Krav från SS-EN ISO 22301:

Organisationen ska

- avgöra vilken kompetens som är nödvändig hos den eller de personer som arbetar åt den och som påverkar dess kontinuitetshanteringsförmåga,
- säkerställa att dessa personer är kompetenta, baserat på lämplig utbildning, upplärning eller erfarenhet,
- vidta åtgärder, där så är tillämpligt, för att införskaffa den nödvändiga kompetensen och utvärdera verkan av de vidtagna åtgärderna,
- bevara lämplig dokumenterad information som belägg för kompetens.

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

Anmärkning: Detta avsnitt gäller kompetens om kontinuitetshanteringsförmåga.

Kompetens som behövs kan exempelvis vara baserad på kunskap och erfarenhet om

- organisationens åtagande,
- lagstiftning inom området,
- kundernas behov,
- operativa processer,
- försörjningskedja och logistik,
- tekniska system,
- risk- och kontinuitetshantering.

För det mesta kommer denna kompetens att finnas tillgänglig i organisationen, men det är viktigt att identifiera eventuella brister som behöver åtgärdas.

SS 22304:2023 (sv)

Om organisationen redan har ett arbetssätt för hur kompetens hanteras kan man utgå från och komplettera detta.

7.3 Medvetenhet

Mål: Kontinuitetshanteringen är en del av organisationskulturen.

Resultat: Berörd personal är medveten om verksamhetens kontinuitetshantering.

Krav från SS-EN ISO 22301:

Personer som arbetar inom eller åt organisationen ska göras medvetna om

- a) kontinuitetspolicyn,
- b) sina bidrag till ett väl fungerande ledningssystem för kontinuitetshantering, inklusive fördelarna med att kontinuitetshanteringens prestanda förbättras,
- c) konsekvenserna av att inte uppfylla kraven i ledningssystemet,
- d) sina egna roller och ansvarsområden före, under och efter störning.

Organisationen bör bestämma sig för vilka aktiviteter som genomförs för att öka medvetenheten gällande kontinuitetshantering. Arbetet bör ske systematiskt och regelbundet. Exempel på aktiviteter kan vara att

- inkludera kontinuitetshantering i introduktionsutbildningar,
- utbilda medarbetare i deras ansvar i kontinuitetsarbetet,
- inkludera kontinuitetshantering på agendan för arbetsmöten där så är lämpligt.

7.4 Kommunikation

Mål: Att skapa effektiv kommunikation och konsultation med berörda parter.

Resultat: Dokumenterade och väl fungerade processer och rutiner finns.

Krav från SS-EN ISO 22301:

Organisationen ska avgöra behovet av sådan intern och extern kommunikation som är relevant för ledningssystemet för kontinuitetshantering, innefattande

- a) vad kommunikationen ska handla om,
- b) när kommunikationen ska ske,
- c) med vem kommunikationen ska ske,
- d) hur kommunikationen ska ske,
- e) vem som ska kommunicera.

Anmärkning: 7.4 rör ledningssystemet, inte kontinuitetslösningarna. Detta avsnitt rör inte heller varning och kommunikation om incidenter, vilket återfinns i 8.4.3.

Här ges ingen kompletterande vägledning då kraven anses vara självförklarande.

7.5 Dokumenterad information

7.5.1 Allmänt

Krav från SS-EN ISO 22301:

Organisationens ledningssystem för kontinuitetshantering ska innefatta

- a) dokumenterad information som krävs enligt detta dokument,
- b) dokumenterad information som organisationen har bestämt är nödvändig för ett väl fungerande ledningssystem för kontinuitetshantering.

Anmärkning: Omfattningen av den dokumenterade informationen för ett ledningssystem för kontinuitetshantering kan variera från en organisation till en annan beroende på

- organisationens storlek och dess typ av aktiviteter, processer, produkter och tjänster samt resurser,
- processernas komplexitet och samverkan,
- personers kompetens.

Här ges ingen kompletterande vägledning då kraven anses vara självförklarande.

7.5.2 Skapande och uppdatering

Krav från SS-EN ISO 22301:

När dokumenterad information skapas och uppdateras ska organisationen säkerställa lämplig

- a) identifiering och beskrivning (t.ex. rubrik, datum, författare eller referensnummer),
- b) form (t.ex. språk, programversion, grafik) och medium (t.ex. papper, elektroniskt format),
- c) granskning och godkännande i fråga om lämplighet och tillräcklighet.

Här ges ingen kompletterande vägledning då kraven anses vara självförklarande.

7.5.3 Styrning av dokumenterad information

Krav från SS-EN ISO 22301:

7.5.3.1 Dokumenterad information som krävs av ledningssystemet för kontinuitetshantering ska styras av detta dokument för att säkerställa att

- a) informationen är tillgänglig och lämplig för användning där den behövs och när den behövs,
- b) informationen är tillräckligt skyddad (t.ex. mot förlust av konfidentialitet, olämplig användning eller förvanskning).

7.5.3.2 För denna styrning av dokumenterad information ska organisationen i tillämplig utsträckning behandla

- a) distribution, åtkomst, inhämtning och användning,
- b) förvaring och bevarande, inklusive bevarande av läsbarhet,
- c) styrning av ändringar (t.ex. versionshantering),
- d) arkivering och gallring.

Dokumenterad information av externt ursprung, som organisationen har bestämt är nödvändig för planering och användning av ledningssystemet för kontinuitetshantering, ska i lämplig utsträckning identifieras och styras.

Anmärkning: Åtkomst kan förutsätta att det tagits ett beslut om behörighet att endast läsa den dokumenterade informationen, eller att både läsa och ändra den dokumenterade informationen.

Här ges ingen kompletterande vägledning då kraven anses vara självförklarande.

8 Verksamhet

8.1 Planering och styrning av verksamheten

Mål: Att planera för en väl fungerande kontinuitetshantering i verksamheten.

Resultat: En styrd och planerad process för kontinuitetshantering finns i verksamheten.

SS 22304:2023 (sv)

Krav från SS-EN ISO 22301:

Organisationen ska planera, införa och styra de processer som behövs för att uppfylla krav och utföra de åtgärder som fastställts i 6.1 genom att

- a) upprätta kriterier för dessa processer,
- b) införa styrning av processerna enligt kriterierna,
- c) i nödvändig utsträckning bevara dokumenterad information för att ge tilltro till att processerna utförts som planerats.

Organisationen ska styra planerade ändringar och granska konsekvenserna av oavsiktliga ändringar samt vid behov vidta åtgärder för att motverka negativa effekter.

Organisationen ska säkerställa styrningen av utkontrakterade processer och försörjningskedjor.

Planering och styrning av verksamheten bör, så långt som möjligt, ske enligt fastställda kriterier. Dessa kriterier bör vara i form av mätbara mål som kan knytas till verksamhetens beslutade kontinuitetsmål, se 6.2.

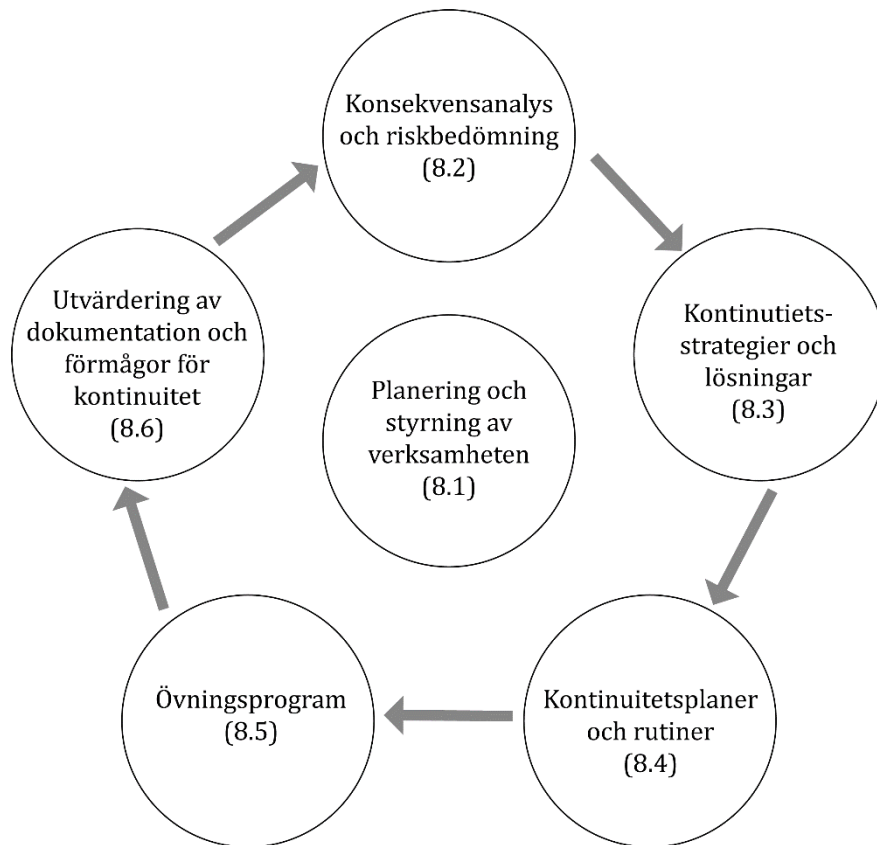
Exempel på sådana kriterier är

- en integrering mellan ledningssystem för kontinuitetshantering och andra processer såsom risk- och krishantering,
- etablerade kommunikationsvägar som kan nyttjas av ledningen och utgöra ett stöd för medarbetarna,
- utsedda roller som ansvarar för uppföljning, kvalitetssäkring och förbättringsåtgärder rörande kontinuitetsprocessen,
- en säkrad tidslinje för kontinuitetsprocessen som är tydligt kommunicerad samt synkroniserad med andra processer såsom verksamhets- och budgetplanering,
- tydliga processteg med mål gällande utfall och vilket mervärde de ger verksamheten.

Organisationen behöver planera, införa och följa upp de åtgärder som behövs för att uppfylla organisationens kontinuitetspolicy och mål samt möta tillämpliga interna och externa behov och krav. Organisationen behöver säkerställa att planerade åtgärder införs i enlighet med verksamhetens övergripande mål.

Organisationen bör arbeta med kontinuitetshantering på ett iterativt sätt i enlighet med PDCA-modellen. Ett exempel på process för detta beskrivs i figur 4. Arbetet bör implementeras i ordinarie verksamhetsstyrning så att ingående delar genomförs i relevanta tidsintervall, t.ex. att samtliga delar genomförs årsvis.

Mycket av informationen som upprättas kan redan finnas inom organisationen, t.ex. är verksamhetsbeskrivning, processbeskrivningar, befintliga rutiner och planer viktiga ingångsvärden.



Figur 4 — Exempel på process för kontinuitetshantering

För att säkerställa effektivitet i arbetet bör en person med erforderligt mandat utses för att koordinera arbetet. En utpekad person inom organisationen bör även ges ett övergripande redovisningsansvar för kontinuitetshanteringsarbetet och dess effektivitet.

8.2 Konsekvensanalys och riskbedömning

8.2.1 Allmänt

Anmärkning: SS-EN ISO 22301 fastställer ingen särskild ordning mellan konsekvensanalys och riskbedömning men följs denna vägledning kan konsekvensanalysen genomföras före och ligger då till grund för riskbedömningen.

Krav från SS-EN ISO 22301:

Organisationen ska

- införa och upprätthålla systematiska processer för konsekvensanalys och riskbedömning för störning,
- revidera konsekvensanalysen och riskbedömningen med planerade intervall och när det sker betydande förändringar i organisationen eller i det sammanhang där den är verksam.

Anmärkning: Organisationen fastställer den ordning i vilken konsekvensanalysen och riskbedömningen utförs.

För att utveckla och införa en systematisk process för konsekvensanalys och riskbedömning bör man så långt som möjligt utgå från de verksamhetsprocesser som redan finns etablerade inom organisationens ledningssystem och integrera dem med varandra. Man bör även ta hänsyn till i vilket sammanhang som verksamheten bedrivs.

Då organisationens verksamhet förändras över tiden behöver konsekvensanalys och riskbedömning uppdateras löpande. Ibland sker förändringar smygande, men det kan även ske hastigt och oväntat.

SS 22304:2023 (sv)

Organisationen bör därför bedriva en aktiv omvärldsbevakning för att skapa goda förutsättningar för att göra konsekvensanalyser och riskbedömningar av god kvalitet.

8.2.2 Konsekvensanalys

Mål: Att analysera verksamheten utifrån vilka konsekvenser en störning eller ett avbrott kan ge. Att identifiera organisationens prioriterade aktiviteter och vilka resurser som är nödvändiga för att utföra dem.

Resultat: Konsekvensanalysen ger en bild över vilka konsekvenser olika avbrott i verksamheten kan få, vilka aktiviteter som är prioriterade och vilka resurser verksamheten behöver för att leverera varor och tjänster.

Krav från SS-EN ISO 22301:

Organisationen ska använda processen för konsekvensanalys för att fastställa verksamhetens prioriteringar och krav för kontinuitetshantering. Processen ska

- a) definiera konsekvenstyper och kriterier som är relevanta för organisationen och dess sammanhang,
- b) identifiera de aktiviteter som behövs för att tillhandahålla produkter och tjänster,
- c) använda de definierade konsekvenstyperna och kriterierna för att bedöma konsekvenserna för verksamheten vid ett avbrott i dessa aktiviteter över tid,
- d) identifiera det tidsspann inom vilken konsekvenserna av att inte återuppta aktiviteterna skulle bli oacceptabla för organisationen,

Anmärkning 1: Detta kan benämnas MTA.

- e) ange prioriterade tidsspann inom den tid som identifieras i d) för att återuppta aktiviteterna till förutbestämd lägsta acceptabel kapacitet,

Anmärkning 2: Detta tidsspann kan benämnas mål för återställningstid.²

- f) använda denna analys för att identifiera prioriterade aktiviteter,
- g) fastställa vilka resurser som behövs för att utföra de prioriterade aktiviteterna,
- h) fastställa beroendeförhållandena, inklusive partners och leverantörer, samt inbördes beroenden mellan prioriterade aktiviteter.

² Mål för återställningstid benämns på engelska som "recovery time objective", RTO.

Omfattningen av konsekvensanalysen bör utgå från de produkter och tjänster som identifierats i 4.3.2 men bör även anpassas efter organisationens behov, typ och storlek. Konsekvensanalysen genomförs lämpligtvis för en produkt eller tjänst i taget.

Det är viktigt att konsekvensanalysen genomförs med personer med olika kompetens för att ge en komplett bild av verksamheten som tillhandahåller produkten eller tjänsten.

Konsekvensanalysen kan genomföras på olika sätt, t.ex. genom workshoppar, intervjuer eller enkäter. Mer information om konsekvensanalysen och möjliga sätt att inhämta information finns beskrivet i SIS-ISO/TS 22317.

Här följer förslag till hur en konsekvensanalys kan genomföras.

a) Definiera konsekvenstyper och kriterier

Konsekvensanalysen börjar med att man definierar de konsekvenstyper som är relevanta för organisationen och dess sammanhang. Konsekvenstyper utgör en kategorisering av de olika typer av konsekvenser som en störning eller ett avbrott i leveransen av en viss vara eller tjänst kan ge upphov till.

Konsekvenstyper kan exempelvis vara liv och hälsa, ekonomi eller förtroende, se tabell 2.

Tabell 2 – Exempel på konsekvenstyper

Konsekvenstyp	Beskrivning
Liv och hälsa	Påverkan på människors liv och hälsa genom skador, dödsfall eller negativa effekter för hälsan.
Ekonomi	Ekonomiska skador till följd av viten, böter, förlorade intäkter eller minskad marknadsandel.
Förtroende	Negativa åsikter hos kunder eller allmänhet, eller skada på varumärke.

Därefter definieras kriterier för respektive konsekvenstyp vilket innebär att besluta om olika konsekvensnivåer, t.ex. försumbar, lindrig, allvarlig eller mycket allvarlig och kriterier för varje sådan nivå som beskriver vad konsekvenserna för respektive nivå innefattar, se tabell 3.

Organisationen kan redan ha definierat konsekvenstyper och kriterier som kan återanvändas i arbetet, t.ex. inom arbete med riskhantering eller informationssäkerhet.

Konsekvenstyperna och kriterierna bör vara beslutade av ledningen och kommunicerade inom organisationen för att säkerställa att bedömningen sker utifrån samma grund och resulterar i en kvalitetssäkrad bedömning.

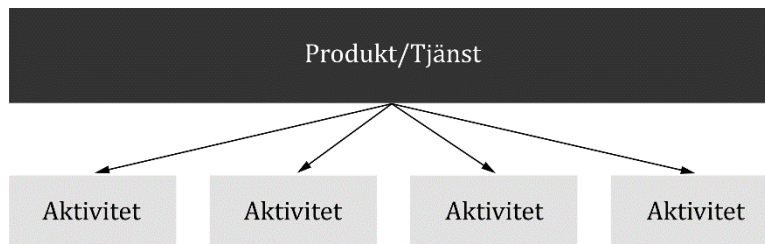
Tabell 3 – Exempel på konsekvenstyper och kriterier

Typ	Försumbar	Lindrig	Allvarlig	Mycket allvarlig
Liv och hälsa	Övergående lindriga obehag.	[antal] lindrigt skadade och lindriga obehag.	[antal] svårt skadade och svåra obehag.	[antal] dödsfall och [antal] svårt skadade.
Ekonomi	Ingen eller obetydlig påverkan på ekonomin.	Begränsad påverkan på delar av organisationens ekonomi. Förlust på [antal] SEK i intäkter eller utgifter. Risk för viten.	Allvarlig påverkan på delar av organisationens ekonomi. Förlust på [antal] SEK och företaget har ålagts viten.	Mycket allvarlig påverkan på hela organisationen ekonomi. Förlust på [antal] SEK [Antal]% av kundfakturor som inte kan betalas och företaget riskerar ekonomiskt obestånd inom [antal] månader.
Förtroende	Liten skada på anseende. Inga negativa inslag i medier.	Viss skada på anseende. Enstaka eller fåtal negativa inslag i rikstäckande medier under [antal] dagar/veckor.	Kortvarig skada på anseende. Flera negativa inslag i rikstäckande medier under [antal] veckor.	Stor skada på anseende. Inslag i merparten av alla viktiga mediekkanaler under [antal] veckor.

Här bör ledningen också besluta om vilka konsekvensnivåer som är tolerabla eller oacceptabla för respektive konsekvenstyp, t.ex. kan ledningen besluta om att allt över försumbar är oacceptabelt för liv och hälsa men att organisationen kan tolerera allvarliga ekonomiska konsekvenser. Detta används som underlag för att bedöma maximal tolerabel avbrottstid.

b) Identifiera aktiviteter

Utgå från de produkter och tjänster som identifierades i 4.3.2. Identifiera de aktiviteter som krävs för att tillhandahålla dessa produkter och tjänster, se figur 5. Organisationen väljer själv hur den vill beskriva aktiviteter, t.ex. som uppgifter som görs eller en process som består av aktiviteter.



Figur 5 — Illustration av hur tillhandahållandet av en produkt eller tjänst kan brytas ner i aktiviteter

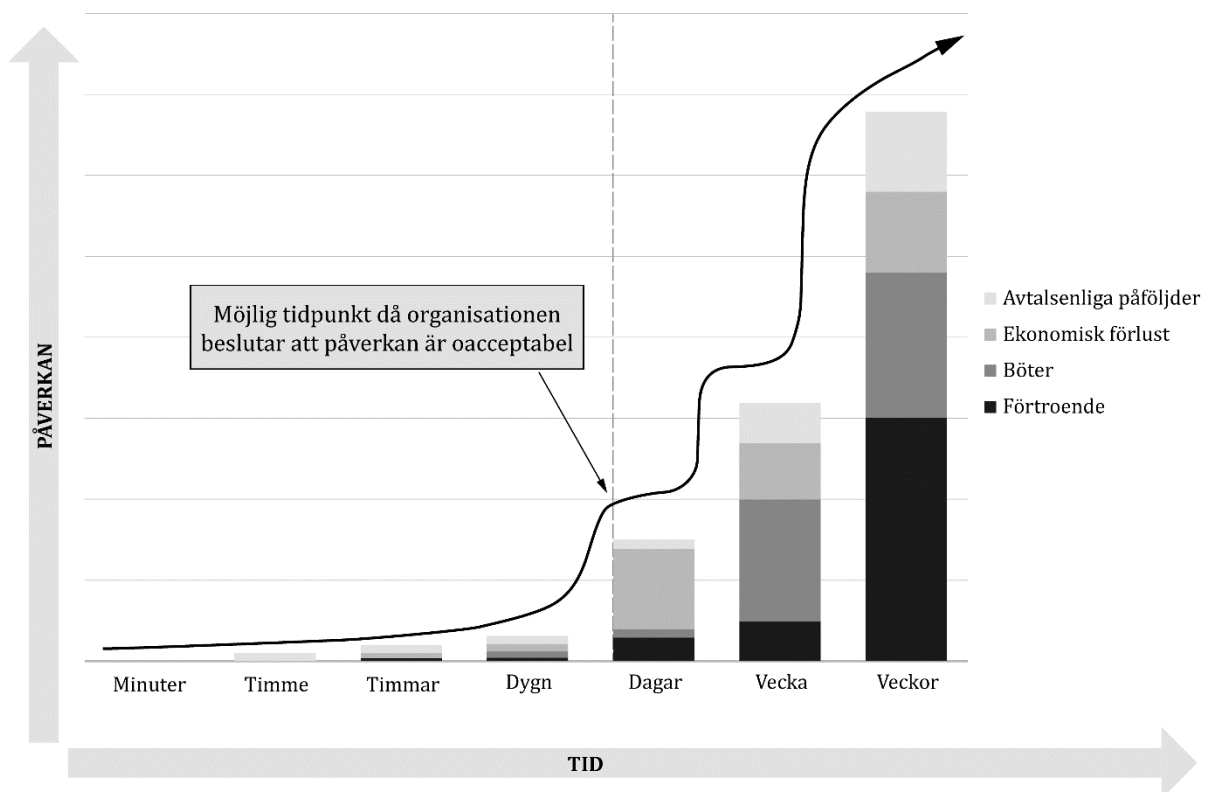
Fastställ vem som har ansvar för respektive aktivitet som analyseras i det fortsatta arbetet.

c) Bedöm konsekvenser av ett avbrott över tid

Bedöm potentiella konsekvenser för verksamheten i händelse av att de identifierade aktiviteterna inte kan upprätthållas. Detta görs för respektive aktivitet och utgår från resultatet av a) *Definiera konsekvenstyper och kriterier*. Bedöm potentiella konsekvenser som avbrottet får för respektive konsekvenstyp och avgör hur lång tid ett avbrott kan fortgå innan en viss konsekvensnivå uppnås.

Resultatet blir en sammanställning över vilka konsekvenser ett avbrott i olika aktiviteter får över tid. Figur 6 utgör ett exempel på hur en sådan sammanställning kan genomföras.

Ett avbrott kan leda till allvarliga konsekvenser inom en viss konsekvenstyp medan det kan få inga eller lindriga konsekvenser för en annan.



Figur 6 — Konsekvensernas utveckling över tid

d) Maximal tolerabel avbrottstid (MTA)

Maximal tolerabel avbrottstid (MTA) är den tid det skulle ta för negativa konsekvenser, som kan uppstå till följd av att inte tillhandahålla en produkt eller en tjänst eller att inte utföra en aktivitet, att bli oacceptabla. Beroende på produkt eller tjänst kan tiden variera från omedelbart till flera veckor eller månader.

För att bestämma maximal tolerabel avbrottstid bör organisationen utgå från resultatet av *a) Definiera konsekvenstyper och kriterier* och ledningens beslut om vilken konsekvensnivå som är oacceptabel för organisationen. Gå därefter till resultatet av *c) Bedöm konsekvenser av ett avbrott över tid* för att få tiden till dess att oacceptabel konsekvens uppnås. Detta tidsspann utgör MTA. Upprepa detta för samtliga aktiviteter.

Om ett avbrott i en aktivitet har olika tid till oacceptabel konsekvens för olika konsekvenstyper så är det den kortaste tiden som utgör aktivitetens MTA.

MTA beror på tidskänsligheten för organisationens produkter och tjänster. Aktiviteter som är tidskänsliga kan behöva specificeras med en högre grad av noggrannhet än aktiviteter som är mindre tidskänsliga.

e) Mål för återställningstid

Mål för återställningstid är den tid inom vilken en aktivitet återupptas till en förutbestämd lägsta tolerabel kapacitet. Innan denna anges behöver alltså först lägsta tolerabla kapacitet för respektive prioriterad aktivitet bestämmas. Detta bör beslutas av högsta ledningen och bland annat ta hänsyn till

- vad som minst behöver levereras för att uppnå organisationens mål,
- avtal och andra överenskommelser kring leverans av den produkt eller tjänst som aktiviteten tillhör,
- annan reglering som organisationen omfattas av.

Därefter anges RTO. RTO bör vara kortare än aktivitetens MTA och hjälper organisationen att identifiera vilka strategier och lösningar som behövs för att korta avbrottstiden och minska konsekvenserna av ett avbrott.

Notera att återställning också kan ske stegvis, t.ex. att 50 % kapacitet nås inom en dag, 75 % kapacitet inom en vecka och 90 % kapacitet inom en månad.

För att säkerställa att prioriterade aktiviteter kan återställas inom angiven tidsram kan RTO även anges för de resurser som är nödvändiga för att säkerställa att aktiviteten fungerar, se g). Här behöver inbördes beroenden mellan resurser tas hänsyn till som exempelvis om resurser behöver återupptas i en viss ordning.

f) Identifiera prioriterade aktiviteter

Identifiering av prioriterade aktiviteter kan t.ex. göras genom att bedöma vilka aktiviteter som

- behöver återupptas inom kortast tid,
- ger upphov till de största konsekvenserna eller
- tar lång tid att återuppta efter ett avbrott.

Detta kan alltså vara aktiviteter med kort MTA eller kort RTO, aktiviteter som vid ett avbrott kan ge upphov till allvarliga konsekvenser, på både kort och lång sikt, eller aktiviteter som av olika anledningar tar lång tid att återuppta efter avbrott. Det kan också handla om aktiviteter som är nödvändiga för att säkerställa att andra aktiviteter fungerar. Beroendeförhållanden identifieras närmare i h).

Arbetet enligt b) till f) kan sammanställas enligt tabell 4.

Tabell 4 – Exempel på tabell för att sammanställa arbete enligt b-f) i konsekvensanalysen

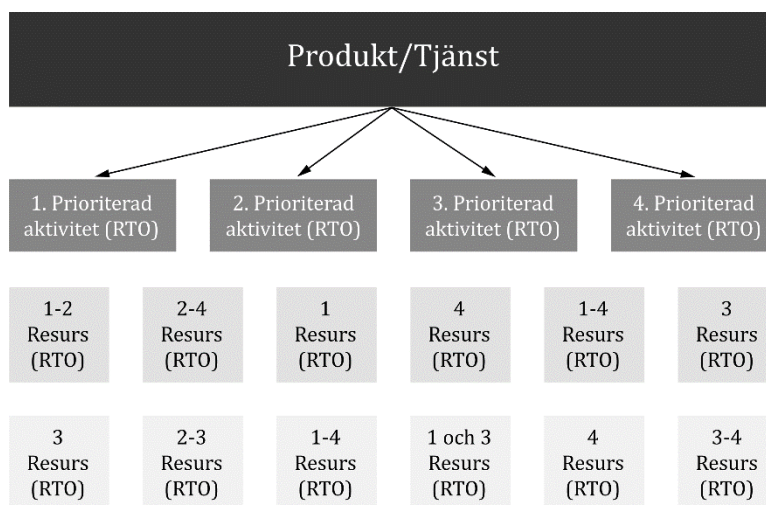
Aktiviteter	Konsekvenser	MTA	RTO	Prioriterad aktivitet?
[namn]	[beskrivning av konsekvenserna över tid utifrån konsekvenstyperna i A]	[identifierad maximalt tolerabel avbrottstid]	[beslutat mål för återställningstid]	[bedömning om aktiviteten är prioriterad eller ej]

g) Identifiera resurser

Identifiera de resurser som är nödvändiga för att utföra de prioriterade aktiviteterna. Det är ofta fördelaktigt att skilja på interna och externa resurser. Exempel på vanliga nödvändiga resurser är

- personal,
- information och data,
- lokaler, arbetsplatser eller andra anläggningar och tillhörande resurser,
- utrustning och förbrukningsmaterial,
- system för informations- och kommunikationsteknik,
- transport och logistik,
- leverantörer,
- teknisk försörjning av el, vatten med mera.

Arbetet enligt g) illustreras i figur 7.



Figur 7 — Sammanställning av b) till g) i konsekvensanalysen med koppling mellan prioriterade aktiviteter och nödvändiga resurser

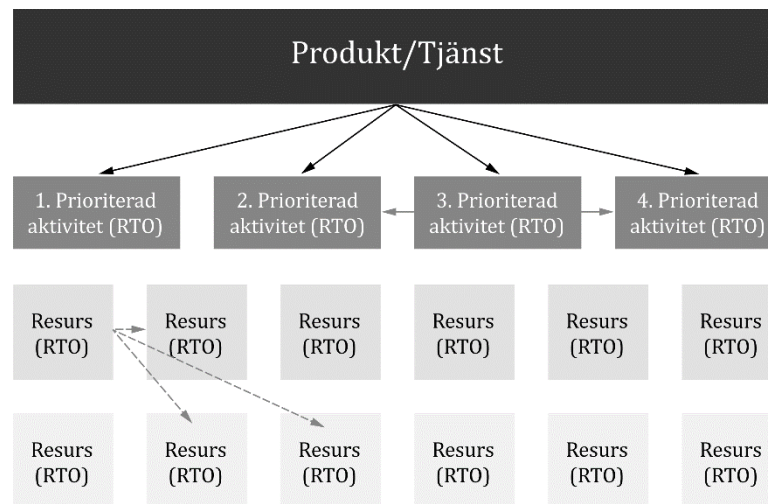
För att underlätta arbetet är det lämpligt att koppla ihop resurserna med de prioriterade aktiviteterna de är nödvändiga för. Ett exempel är att numrera de prioriterade aktiviteterna enligt figur 7.

När resurser kopplade till information och data identifieras bör hänsyn tas till att den information och de uppgifter som behövs för att kunna återuppta aktiviteten är aktuella och användbara. Detta kallas mål för återställningspunkt.

h) Identifiera beroendeförhållanden

Identifiera beroenden mellan resurser och inbördes mellan prioriterade aktiviteter, se figur 8.

Det är fördelaktigt att även resurserna tilldelas RTO. När RTO anges för resurserna bör hänsyn tas till beroendeförhållanden, t.ex. om resurser behöver återupptas i en viss ordning eller om en resurs berör flera aktiviteter. Det innebär att resurserna kan ges olika RTO och får inte överstiga aktivitetens MTA. Om en resurs berör fler än en aktivitet är det aktiviteten med kortast RTO som blir styrande för när resursen behöver vara återställd. Organisationen bör också fastställa till vilken kapacitet de nödvändiga resurserna behöver återupptas.



Figur 8 — Beroendeförhållanden i konsekvensanalysen

8.2.3 Riskbedömning

Mål: Att bidra till en förståelse för risker som kan leda till avbrott i organisationens prioriterade aktiviteter.

Resultat: Ett beslutsunderlag för vilka risker som behöver åtgärdas finns.

Krav från SS-EN ISO 22301:

Organisationen ska införa och underhålla en process för riskbedömning.

Anmärkning: Processen för riskbedömning behandlas i ISO 31000.

Organisationen ska

- identifiera risker för avbrott i organisationens prioriterade aktiviteter och deras nödvändiga resurser,
- analysera och utvärdera de identifierade riskerna,
- fastställa vilka risker som behöver åtgärdas.

Anmärkning: Risker i detta underavsnitt avser avbrott i verksamhetens aktiviteter. Risker och möjligheter relaterade till ledningssystemets effektivitet behandlas i 6.1.

Riskbedömningen bidrar med en strukturerad process för att identifiera, analysera och utvärdera riskerna för störning eller avbrott i organisationens prioriterade aktiviteter och dess nödvändiga resurser. Denna process behandlas i SS-ISO 31000:2018. Den samlade bedömningen ligger till grund för vilka risker som behöver åtgärdas. Eftersom prioriterade aktiviteter och dess nödvändiga resurser identifieras i konsekvensanalysen, se 8.2.2, bör riskbedömningen genomföras efter konsekvensanalysen.

SS 22304:2023 (sv)

Arbetet med riskbedömningen kan genomföras på olika sätt, exempelvis genom frågeformulär, intervjuer, scenarioövningar och workshoppar.

Om organisationen har olika grupper med ansvar för kontinuitetshantering och riskhantering bör riskbedömningen genomföras tillsammans. På så vis kan både rätt kompetens och lärdomar från tidigare utförda riskbedömningar nyttjas.

Här följer förslag till hur en riskbedömning kan genomföras.

Riskbedömningen bör besvara följande frågor:

- Vilka risker finns som kan leda till störning eller avbrott i organisationens prioriterade aktiviteter?
- Vilka risker finns som kan leda till att nödvändiga resurser blir otillgängliga?
- Vilken befintlig redundans och andra åtgärder finns för nödvändiga resurser?
- Om en risk inträffar som gör en nödvändig resurs otillgänglig, hur är organisationens förmåga att upprätthålla återställningstiden?
- Vilka risker behöver åtgärdas?

a) Riskidentifiering

Riskidentifieringen utgår ifrån de prioriterade aktiviteterna och resurserna identifierade i 8.2.2 f) och g). Riskidentifieringen besvarar vilka risker det finns som kan leda till störning eller avbrott i respektive aktivitet eller ett bortfall av en nödvändig resurs.

Som ett stöd vid riskidentifiering kan vanliga riskkällor användas. Exempel på riskkällor är

- brand,
- naturolycka,
- personalbrist,
- strömavbrott,
- tekniskt fel,
- obehörig åtkomst,
- IT-attack.

Avbrott i prioriterade aktiviteter orsakas ofta av att en eller flera av aktivitetens nödvändiga resurser blir otillgängliga. Att fokusera på resurserna kan därför i många fall vara tillräckligt. Riskidentifiering kan exempelvis genomföras genom att för varje identifierad nödvändig resurs fråga sig vad som kan orsaka bortfall av denna?

b) Riskanalys och riskutvärdering

Riskanalysen syftar till att få en större förståelse för risken och dess potential att orsaka avbrott i organisationens prioriterade aktiviteter. För att lyckas med detta är det viktigt att ta hänsyn till sårbarheter inom organisationen samt befintlig redundans.

Sårbarhet kan beskrivas som omständighet som gör organisationen mer känslig för en viss risk. Exempel på sårbarheter är

- avsaknad av eller bristande redundans,
- låg lagerhållning,
- dålig säkerhetskultur,
- låg nivå på brandskydd,
- bristande informationssäkerhet,
- endast en underleverantör av en viss nödvändig resurs (single sourcing).

Som exempel innebär avsaknad av redundant elförsörjning till nödvändig och elberoende teknisk utrustning att organisationen är mer känslig för strömavbrott.

Utgå från de identifierade riskerna i a),

- vilka sårbarheter gör organisationen känslig för respektive risk?
- vilken befintlig redundans eller andra åtgärder finns för att kontrollera risken?

Redundans kan handla om befintliga reservlösningar som reservkraft, reservlokaler, dubbla IT-system eller vikariebank för personal. Andra åtgärder kan vara brandskydd eller anti-virusprogram.

För varje aktivitet och resurs bedöms förmågan att RTO kan uppfyllas. Här räknas befintlig redundans och andra skyddsåtgärder in i denna bedömning.

Riskbedömningen ger indikationer om vilka risker och sårbarheter som behöver åtgärdas först och var redundansen behöver öka.

Kontinuitetshantering syftar till att skapa en förmåga att upprätthålla leverans av produkter och tjänster oavsett vad som inträffar. Vidare är det i princip omöjligt att förutse alla risker som kan leda till avbrott. Däremot går det att skapa en förmåga att återuppta prioriterade aktiviteter till en lägsta tolerabel nivå. Därmed är sannolikheten för själva risken som kan leda till avbrott mindre intressant utan det är i stället sannolikheten att kunna återuppta aktiviteten eller att återställa resursen som bör användas vid riskvärdering och beslutsfattande om vilka risker som behöver åtgärdas. Denna sannolikhet är direkt kopplad till förmågan att upprätthålla mål för återställningstid.

c) Riskhanteringsåtgärder

Riskhanteringsåtgärder kan genomföras för att antingen reducera sannolikheten för att risken inträffar eller begränsa konsekvenserna om den inträffar. I detta fall handlar det om att genomföra åtgärder för att minska sannolikheten att mål för återställningstid överskrids. Det kan handla om åtgärder som minskar organisationens sårbarheter för avbrott eller att på andra sätt stärka redundans för nödvändiga resurser.

Utgå från genomförd riskanalys och utvärdering i b). För vilka aktiviteter och resurser är sannolikheten att mål för återställningstid överskrids störst? Vilka åtgärder krävs för att reducera denna sannolikhet? Särskilt fokus bör läggas på aktiviteter med hög prioritet eller resurser som tar lång tid att återställa.

En mall för enklare riskbedömning återfinns i tabell 5.

Tabell 5 – Exempel på mall för riskbedömning

	Prioriterad aktivitet								
Nödvändig resurs (RTO)	Risk	Sårbarhet	Befintlig redundans	Förmåga att upprätthålla RTO				Är risken tolerabel, ja eller nej?	Prioritet
				God	God med vissa brister	Bristfällig	Mycket bristfällig		

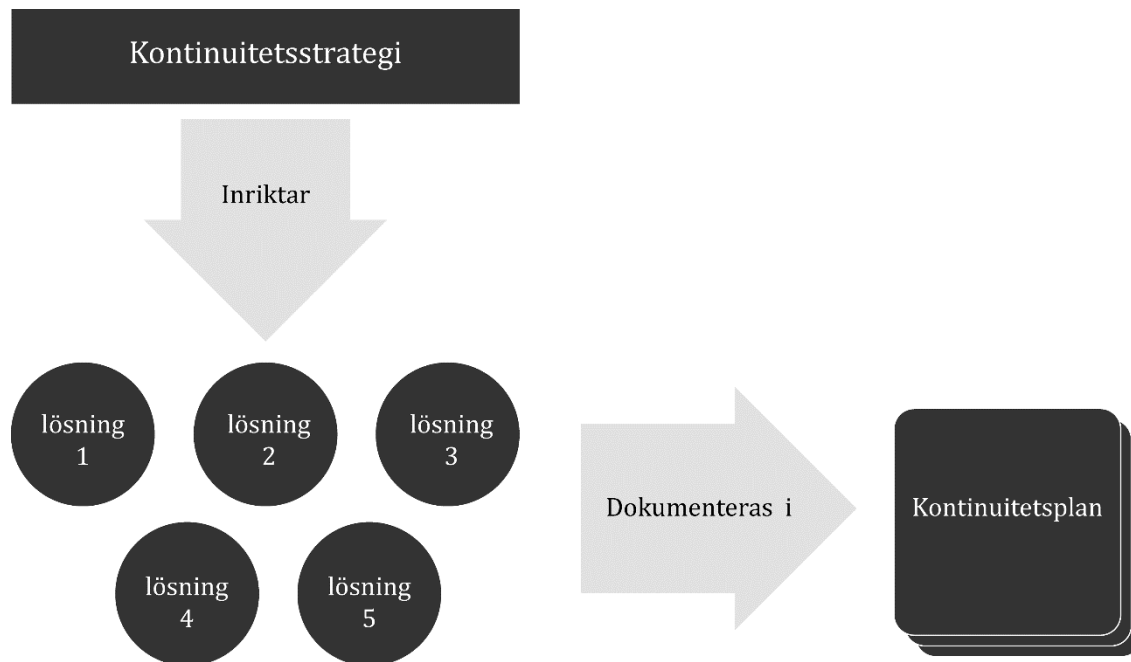
8.3 Kontinuitetsstrategier och lösningar

8.3.1 Allmänt

Krav från SS-EN ISO 22301:

Utifrån konsekvensanalysen och riskbedömningen ska organisationen identifiera och välja kontinuitetsstrategier som beaktar alternativ före, under och efter avbrott. Kontinuitetsstrategierna ska bestå av en eller flera lösningar.

En kontinuitetsstrategi anger en inriktning för vilka lösningar som implementeras för att uppfylla organisationens krav på kontinuitet. Lösningarna kan behandla olika tillvägagångssätt, metoder, rutiner och åtgärder som kan vidtas. Det kan finnas flera olika lösningar som tillämpas för en kontinuitetsstrategi. När man sedan bestämt vilka lösningar som organisationen tillämpar så dokumenteras dessa i en kontinuitetsplan, se figur 9.



Figur 9 — Illustration av förhållandet mellan kontinuitetsstrategi, kontinuitetslösning och kontinuitetsplan

En kontinuitetsstrategi för användning *före* en störning syftar till att förebygga eller minska sannolikheten för störningen, t.ex. genom att fördela prioriterade aktiviteter och eller resurser på olika fysiska platser. Detta minskar sannolikheten för en störning i denna aktivitet trots en störning på en av platserna.

En kontinuitetsstrategi för användning *under* en störning syftar till att få så små störningar som möjligt i verksamheten, t.ex. genom att installera reservkraft, lagerhålla kritiska resurser eller att ha rutiner för alternativa arbetssätt.

En kontinuitetsstrategi för användning *efter* en störning syftar till att lindra konsekvenserna av störningen, t.ex. genom att ha försäkringar som reducerar den ekonomiska förlusten.

8.3.2 Identifiering av strategier och lösningar

Resultat: Att lämpliga kontinuitetsstrategier och lösningar är identifierade utifrån organisationens behov.

Mål: Organisationen har utifrån sina förutsättningar och behov identifierat väl avvägda strategier och lösningar för sin kontinuitetshantering.

Krav från SS-EN ISO 22301:

Identifiering ska vara baserad på i vilken utsträckning som strategier och lösningar:

- a) uppfyller kraven för att fortsätta med och återuppta prioriterade aktiviteter inom de identifierade tidsramarna och till en fastställd kapacitet,
- b) skyddar organisationens prioriterade aktiviteter,
- c) minskar sannolikheten för störning,
- d) förkortar tiden för störning,
- e) begränsar störningens konsekvens på organisationens produkter och tjänster,
- f) möjliggör tillgång till lämpliga resurser.

Att identifiera kontinuitetsstrategier och lösningar innebär att inventera förslag på strategier och ingående lösningar som är lämpliga för att uppfylla organisationens kontinuitetsmål. Det är viktigt att tänka brett och lista alla tänkbara strategier och lösningar. För exempel på kontinuitetsstrategier se tabell 6.

Tabell 6 – Exempel på kontinuitetsstrategier

Kontinuitetsstrategier	Beskrivning av strategi
<i>Differentiera</i>	innebär att aktiviteter eller resurser sprids på minst två geografiska platser, så att en plats kan fortsätta fungera även om den andra platsen utsätts för störning.
<i>Replikera</i>	innebär en spegling av utrustning eller resurser på annan plats där personalen kan återuppta verksamheten vid störning.
<i>Omlokalisera</i>	innebär att en eller delar av leverans eller prioriterad aktivitet flyttas, t.ex. inom organisationen eller till en annan extern part. Det kan också vara att etablera alternativa arbetsplatser, t.ex. i reservlokaler eller på kontorshotell.
<i>Omfördela resurser</i>	innebär att resurser flyttas eller omfördelas för att nyttjas bättre, t.ex. kan personal flyttas till en annan plats eller till en annan prioriterad aktivitet inom organisationen eller till en extern part.
<i>Skapa redundans</i>	innebär att organisationen ökar alternativ kapacitet för prioriterade aktiviteter eller dess nödvändiga resurser i syfte att minska risken för störning eller öka sannolikheten för att nå målet för återställningstiden, t.ex. genom att etablera alternativa processer, lagerhållning eller reservkapacitet.
<i>Utveckla alternativa arbetssätt</i>	innebär att tillfälliga arbetssätt utvecklas för att kunna upprätthålla eller ersätta prioriterade aktiviteter eller resurser, t.ex. genom manuella rutiner eller förändring i processer.
<i>Teckna försäkring</i>	innebär att organisationen tecknar en försäkring som kan ge ekonomisk ersättning efter ett avbrott. Viktigt är dock att försäkringar inte täcker förluster i form av varumärke, rykte eller marknadsandelar. En försäkring bör därför användas tillsammans med andra strategier.
<i>Anlita extern part</i>	innebär att avtala extern aktör som snabbt kan komma på plats för att återställa prioriterade aktiviteter eller resurser.
<i>Hantera förtroende</i>	innebär att organisationen har en tydlig process för att hantera kommunikationen vid en störning, t.ex. genom att ta fram kommunikationsplan och kontaktlistor.
<i>Tolerera risk</i>	innebär att organisationen beslutar sig för att tolerera risk och tillhörande konsekvenser mot en prioriterad aktivitet eller nödvändig resurs.

Lösningarna utgår från strategin och bör vara så konkreta som möjligt. För exempel på kontinuitetslösningar för olika typer av resurser se tabell 7. Lösningarna beskrivs och dokumenteras

SS 22304:2023 (sv)

sedan i kontinuitetsplaner.

Tabell 7 – Exempel på kontinuitetslösningar för olika typer av resurser

Resurs	Exempel på kontinuitetslösningar
Personal	– Anställa ny personal. – Ta in vikarier från bemanningsföretag. – Omfördela personal från andra delar av organisationen. – Planera för kunskapsöverföring för att minska nyckelpersonsberoende.
Information och data	– Utföra regelbunden säkerhetskopiering. – Använda molntjänster. – Utföra sekretessklassificering av all information.
Fysisk infrastruktur	– Förberedda alternativa lokaler. – Hyra plats på kontorshotell. – Arbeta på distans. – Spegla arbetsplatser på olika verksamhetsorter. – Tillhandahålla elaggregat för reservkraft. – Tillhandahålla dubbla elanslutningar från olika distributionsnät. – Tillhandahålla dubbla vattenintag från olika distributionsnät. – Tillhandahålla alternativa lösningar för datakommunikation (fast och trådlös).
Utrustning och förbrukningsmaterial	– Möjliggöra lagerhållning av insatsvaror och reservdelar. – Teckna avtal om prioriterad tillgång till nödvändiga resurser med leverantörer.
System för informations- och kommunikationsteknik	– Tillhandahålla reservwebbplats hos annan leverantör. – Tillhandahålla alternativa mobiloperatörer. – Använda sociala medier. – Sammanställa telefonlistor med anställdas privata telefonnummer.
Transport och logistik	– Teckna avtal med flera olika transportföretag. – Upprätthålla egna transportresurser.
Ekonomi	– Vidhålla likviditetsbuffert för brådskande utgifter. – Teckna försäkringar för stora fysiska värden. – Teckna avtal för nödlån med kreditinstitut.
Partners och leverantörer	– Säkerställa leveranssäkerhet genom avtal t.ex genom att inkludera SLA:er i dessa avtal. – Använda fler än en leverantör. – Genomföra regelbunden revision av andra aktörers kontinuitetshantering. – Genomföra gemensamma krigsövningar med leverantörer. – Inventera alternativa leverantörer.
Anmärkning: SLA står för Service Level Agreement, vilket vanligtvis kallas för ett servicenivåavtal eller SLA-avtal på svenska.	

8.3.3 Val av strategier och lösningar

Mål: Att välja lämpliga kontinuitetsstrategier och lösningar.

Resultat: Valda kontinuitetsstrategier och lösningar grundade på genomförda konsekvensanalyser och riskbedömningar.

Krav från SS-EN ISO 22301:

Valet ska vara baserat på i vilken utsträckning som strategier och lösningar

- a) uppfyller kraven för att fortsätta med och återuppta prioriterade aktiviteter inom de identifierade tidsramarna och till den fastställda lägsta acceptabla kapaciteten,
- b) beaktar graden och typen av risk som organisationen eventuellt kan utsätta sig för,
- c) beaktar tillhörande kostnader och nyttor.

Vid val av strategier och lösningar bör organisationen utgå från strategier och lösningar identifierade i 8.3.2. I enlighet med a) utgör valda strategier och lösningar i första hand att tillse att prioriterade aktiviteter kan återupptas inom de i 8.2.2 identifierade tidsramarna och till lägsta fastställda acceptabla kapacitet.

Organisationen bör enligt b) även ta hänsyn till i 8.2.3 genomförd riskbedömning och att valda strategier och lösningar minskar sannolikheten att överskrida mål för återställningstid. Man bör även beakta de nya risker som valda strategier och lösningar medför.

Organisationen bör enligt c) även beakta hur genomförbar och lämplig åtgärden är utifrån kostnad och nytta. Detta kan bland annat göras genom att välja strategier och lösningar som kan användas av flera delar av organisationen.

Organisationen bör dokumentera val av kontinuitetsstrategier och lösningar inklusive motivering till varför en viss strategi och lösning väljs framför andra. Detta inkluderar även de fall där organisationen väljer att inte implementera en viss strategi eller lösning.

Exempel: tillverkningsindustri

Ett företag inom tillverkningsindustrin producerar tre olika produkter (1, 2 och 3) vid tre olika produktionsanläggningar (A, B och C). Produkt 1 utgör 90 % av företagets försäljning och produceras idag vid anläggning A. På grund av den höga efterfrågan på produkt 1 har ledningen utifrån genomförd konsekvensanalys valt ut produktion av produkt 1 som en prioriterad aktivitet.

För att minska sårbarheten för avbrott i produktionen av produkt 1 har företaget, som kontinuitetsstrategi, valt att omfördela produktionen av produkten så att den produceras både vid produktionsanläggning A och B.

För att uppfylla beslutad strategi väljs följande lösningar:

- Investering i ny produktionslina vid produktionsanläggning B.
- Rekrytering och utbildning av personal vid produktionsanläggning B.
- Utökning av lager och logistik vid produktionsanläggning B.

8.3.4 Resurskrav

Mål: Att fastställa vilka resurser som krävs för att genomföra valda lösningar.

Resultat: Resurskrav finns fastställda.

SS 22304:2023 (sv)

Krav från SS-EN ISO 22301:

Organisationen ska fastställa resurskraven för att införa de valda lösningarna för kontinuitetshantering. De typer av resurser som beaktas ska inkludera men inte vara begränsade till

- a) människor,
- b) information och data,
- c) fysisk infrastruktur såsom byggnader, arbetsplatser eller andra anläggningar och tillhörande resurser,
- d) utrustning och förbrukningsmaterial,
- e) system för informations- och kommunikationsteknik (IKT),
- f) transport och logistik,
- g) ekonomi,
- h) partners och leverantörer.

När resurskrav fastställs bör organisationen utgå från befintliga resurser som den förfogar över. Organisationen bör se över om det krävs specialutrustning eller om det finns komponenter som har lång leveranstid, om lager eller specialavtal behöver övervägas med mera.

Exempel: resurskrav

Strategi kopplat till lokaler: omlokalisera

Lösning 1: utnyttja egna reservlokaler

Resurskrav:

- Reservlokal, vidare bör det finnas rutin för förflyttning till reservlokal samt att reservlokalen utrustas med tillgång till
 - erforderlig information och data,
 - erforderlig utrustning och förbrukningsmaterial,
 - erforderliga IT-system.

Lösning 2: personal arbetar hemifrån

Resurskrav:

- Dator (inklusive annan utrustning: skärm, headset, tangentbord, datormus).
- Säker och tillräcklig internetuppkoppling.
- Utrustning för arbetsplats i hemmet (arbetsmiljö, kollektivavtal med mera).

Lösning 3: avtal om tillgång till lokaler hos tredje part

Resurskrav:

- Inventera resursbehov i lokalerna (kommunikationer med mera).
- Inventera säkerhetsbehov.
- Upphandla/ingå avtal med lämplig aktör.

8.3.5 Implementering av lösningar

Mål: Att valda kontinuitetslösningar är en del av organisationens vardag.

Resultat: Kontinuitetslösningar är implementerade i organisationens verksamhet.

Krav från SS-EN ISO 22301:

Organisationen ska införa och upprätthålla valda kontinuitetslösningar så att de kan aktiveras när så behövs.

För att införa och upprätthålla valda kontinuitetslösningar med tillhörande resurskrav bör åtgärder identifieras och genomföras. Åtgärderna bör dokumenteras och innehålla information om t.ex. prioritet, kostnad och tidplan för genomförandet. För att säkerställa att åtgärderna genomförs och implementeras i den ordinarie verksamheten är det lämpligt om de inkluderas i organisationens ordinarie processer för t.ex. ekonomi och verksamhetsplanering.

I implementeringsarbetet bör organisationen beakta vilka lösningar som behöver prioriteras först med hänsyn till bland annat resultatet av riskbedömningen enligt 8.2.3, ledtider för genomförandet av olika lösningar och ekonomin.

8.4 Kontinuitetsplaner och rutiner

8.4.1 Allmänt

Mål: Att upprätta, införa och underhålla rutiner för att hantera störningar.

Resultat: Dokumenterade rutiner för att säkerställa fortsatt verksamhet och hantering av störning finns.

Krav från SS-EN ISO 22301:

Organisationen ska införa och upprätthålla en hanteringsstruktur för att möjliggöra tidig varning och kommunikation med relevanta berörda parter. Strukturen ska också tillhandahålla planer och rutiner för att leda organisationen under en störning. Planerna och rutinerna ska användas när det behövs för att aktivera kontinuitetslösningar.

Anmärkning Det finns olika typer av rutiner som inbegriper kontinuitetsplaner.

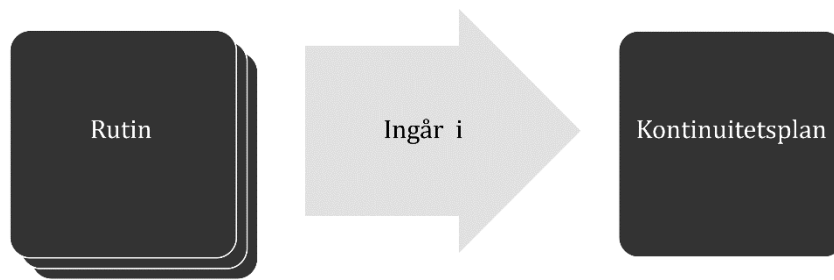
Organisationen ska identifiera och dokumentera kontinuitetsplaner och rutiner baserat på utfallet av de valda strategierna och lösningarna.

Rutinerna ska

- a) vara specifika gällande de omedelbara åtgärder som ska vidtas vid en störning,
- b) vara flexibla för att agera på föränderliga inre och yttre förhållanden vid en störning,
- c) fokusera på konsekvensen av incidenter som potentiellt leder till en störning,
- d) vara effektiva genom införande av lämpliga lösningar för att minimera konsekvenser,
- e) tilldela roller och ansvar.

En hanteringsstruktur består av ett eller flera team med ansvar för att hantera störningar. Upprättade kontinuitetsplaner används som vägledning för att vidta åtgärder.

En kontinuitetsplan är dokumenterad information som vägleder en organisation att hantera en störning och återuppta, återhämta och återställa leveransen av produkter och tjänster i överensstämmelse med organisationens mål för kontinuitetshantering. Kontinuitetsplanen innehåller en eller flera rutiner, se figur 10, som bland annat beskriver vilka åtgärder som vidtas vid en störning för att minimera konsekvenserna för verksamheten. Upprättande av kontinuitetsplaner beskrivs vidare i 8.4.4.



Figur 10 — Illustration av förhållandet mellan rutiner och kontinuitetsplan

8.4.2 Hanteringsstruktur

Mål: Att skapa förutsättningar för organisationen att kunna hantera störningar.

Resultat: Ett etablerat ramverk för att agera på incidenter finns.

Krav från SS-EN ISO 22301:

8.4.2.1 Organisationen ska införa och upprätthålla en struktur som utser en eller flera team som har ansvar för att hantera störningar.

8.4.2.2 Roller och ansvarsområden för respektive team samt relationerna mellan teamen ska vara tydliga.

8.4.2.3 Tillsammans ska teamen ha kompetens för att

- a) bedöma karaktär och omfattning av en störning och dess potentiella konsekvenser,
- b) bedöma konsekvensen i förhållande till fördefinierade tröskelvärden för att avgöra om formell åtgärd krävs,
- c) vidta lämplig hantering för att upprätthålla kontinuiteten,
- d) planera åtgärder som behöver vidtas,
- e) fastställa prioritering (med personsäkerhet som högsta prioritet),
- f) övervaka konsekvenserna av en störning och organisationens hantering,
- g) aktivera kontinuitetslösningar,
- h) kommunicera med relevanta berörda parter, myndigheter och medier.

8.4.2.4 För varje team ska det finnas

- a) identifierade medarbetare och ersättare för dessa, med ansvar, befogenhet och kompetens för att utföra det som åligger dem i deras utsedda roller,
- b) dokumenterade rutiner som vägleder deras åtgärder, se 8.4.4, inklusive sådana för aktivering, genomförande, samordning och kommunikation för hanteringen

En hanteringsstruktur kan införas genom att utse ett eller flera team med ansvar att hantera störning i prioriterade aktiviteter.

I varje team tydliggörs roller och ansvarsområden, se exempel i tabell 8. Organisationen bör anpassa rollerna och kompetensen efter respektive kontinuitetslösning i organisationens kontinuitetsplaner.

Tabell 8 – Exempel på roller och ansvarsområden

Roll	Ansvarsområde
Kontinuitetsansvarig	Ansvarar för aktivering av relevanta kontinuitetsplaner och delegerar uppgifter i enlighet med dessa. I detta ansvar ingår att kunna följa effekterna av en incident som kan leda till störning och fatta beslut om åtgärd när fördefinierade tröskelvärden överskrids, så att kontinuitetsmål och mål för återställningstid, uppfylls. Ett tröskelvärde kan t.ex. vara att lagerhållning av en viss komponent aldrig får underskrida ett visst antal.
Operativt ansvarig	Ansvarar för hur den operativa verksamheten bedrivs, t.ex. i en tillverkningsindustri innebär detta bland annat ansvar att styra produktionen och vid behov prioritera vilka produkter som tillverkas med mera.
Informationsansvarig	Ansvarar för att inhämta information nödvändig för att fatta beslut och dela denna till övriga i teamet.
Kommunikationsansvarig	Ansvarar för intern och extern kommunikation. Vad kommuniceras, hur (t.ex. i vilka kanaler) kommuniceras det och när kommuniceras det.
Dokumentationsansvarig	Ansvarar för att dokumentera vad som har hänt vid en störning, vilka beslut som fattas och vilka åtgärder som vidtas. Denna dokumentation kan sedan användas av kommunikationsansvarig och för att i efterhand lära av de erfarenheter som införskaffades under störningen.
IT-ansvarig	Ansvarar för att eventuella verksamheter som är beroende av IT-system upprätthålls eller ges alternativ.

I vissa fall kan samma person ha fler än en roll.

I det fall organisationen har en befintlig krishanteringsgrupp bör man utvärdera huruvida denna även kan användas för att hantera störning.

8.4.3 Varning och kommunikation

Mål: Att skapa förutsättningar till att upptäcka, övervaka och kommunicera incidenter.

Resultat: Upprättade, införda och underhållna rutiner finns för att upptäcka, övervaka och kommunicera incidenter.

Krav från SS-EN ISO 22301:

8.4.3.1 Organisationen ska dokumentera och upprätthålla rutiner för att

- kommunicera internt och externt med relevanta berörda parter, inklusive om vad, när, med vem och hur kommunikationen ska ske,

Anmärkning: Organisationen kan dokumentera och upprätthålla rutiner för hur och under vilka omständigheter organisationen kommunicerar med anställda och deras närmsta anhöriga.

- ta emot, dokumentera och besvara kommunikation från berörda parter inklusive privata och offentliga aktörer,
- säkerställa tillgänglighet till relevanta kommunikationsmedel vid en störning,
- underlätta strukturerad kommunikation med blåljusenheter,

Nationell fotnot: Här ingår t.ex. räddningstjänst, polis, ambulans men även väktare eller intern nödlägesorganisation.

- tillhandahålla uppgifter om organisationens mediehantering efter en incident, inklusive en kommunikationsstrategi,
- dokumentera information om avbrottet, vilka åtgärder som vidtogs och vilka beslut som fattades.

8.4.3.2 Där så är tillämpligt ska även följande beaktas och implementeras

SS 22304:2023 (sv)

- a) uppmärksamma berörda parter som potentiellt påverkas av ett faktiskt eller överhängande avbrott,
- b) säkerställa lämplig samordning och kommunikation mellan flera hanterande organisationer.

Varnings- och kommunikationsrutinerna ska tillämpas som en del av organisationens övningsprogram som beskrivs i 8.5.

För att kunna hantera en händelse effektivt bör organisationen snabbt kunna kommunicera med både interna och externa berörda parter. Detta innebär att tydliga rutiner för hur detta sker måste finnas på plats. De mest centrala frågorna handlar om vad, när, med vem och hur organisationen ska kommunicera. Eftersom ett avbrott kan påverka kommunikationsvägarna bör organisationen säkerställa att det finns olika sätt att kommunicera på.

Med varning och kommunikation avses kommunikation om verksamhetens kontinuitet vid olika skeden av en händelse. Organisationen bör tydligt förstå vikten av att tidigt kommunicera att en händelse kan komma att ge avbrott i leveranser och att hålla berörda parter informerade vid ett avbrott. För vägledning kring varning till allmänheten, se ISO 22322.

Kommunikationen bör kunna nå alla berörda parter, vilket behöver vara en del av organisationens rutiner. Ibland kan det finnas grupper med särskilda behov där kommunikationen behöver anpassas, t.ex. språk och kommunikationsvägar.

Rutinerna bör tydliggöra vilken befattning eller funktion som ansvarar för kommunikation med de olika berörda parterna, särskilt medier. Det är också viktigt att samordna uppgifter och budskap vid kommunikationsinsatser internt och externt.

En enkel rutin för kommunikation kan innehålla svar på följande frågor:

- Vad bör kommuniceras?
- När bör det kommuniceras?
- Till vem bör kommunikationen gå?

Utgå från identifierade berörda parter för att ge en målgruppsanpassad kommunikation. Berörda parter kan vara såväl interna som externa.

- Vilka kommunikationskanaler bör användas?
- Vem är avsändaren och vem ser till att kommunikationen sker?

För exempel på enkel rutin för kommunikation se tabell 9.

Tabell 9 – Exempel på enkel rutin för kommunikation

BERÖRD PART	EXTERN KONTAKTPERSON	INTERN ANSVARIG	KOMMUNIKATIONS- METOD	VAD SOM KOMMUNICERAS
LEVERANTÖRER	Namn, kontaktuppgifter	Inköp	Telefon, e-post, hemsida & medier	Avbrott i produktion eller leverans och som påverkar inköpsmängder
STÖRRE KUNDER	Namn, kontaktuppgifter	Marknad	Telefon, e-post, hemsida & medier	Avbrott i inköp, produktion eller leverans och som påverkar vilka produkter eller mängden av produkter som kan levereras
ALLMÄNHET (KUND)	Ej applicerbart	Marknad	Hemsida, medier och sociala medier	Avbrott i inköp, produktion eller leverans och som påverkar vilka produkter eller mängden av produkter som kan levereras
BLÅLJUSENHETER	Ej applicerbart	Säkerhet		
MEDIER	Ej applicerbart	Kommunikat ion		

8.4.4 Kontinuitetsplaner

Mål: Att skapa och sammanställa dokumenterade kontinuitetsplaner.

Resultat: Dokumenterade kontinuitetsplaner med nödvändigt innehåll finns för att upprätthålla, hantera och återställa verksamheten vid störningar eller avbrott.

Krav från SS-EN ISO 22301:

8.4.4.1 Organisationen ska dokumentera och underhålla kontinuitetsplaner och rutiner. Kontinuitetsplanerna ska tillhandahålla vägledning och information för att hjälpa teamen att hantera ett avbrott och för att hjälpa organisationen med åtgärder och återställning.

8.4.4.2 Tillsammans ska kontinuitetsplanerna innehålla

- a) uppgifter om vilka åtgärder som teamen ska vidta för att
 - 1) upprätthålla eller återställa prioriterade aktiviteter inom förutbestämda tidsramar,
 - 2) övervaka konsekvensen av avbrottet och organisationens hantering av det,
- b) hänvisning till de fördefinierade tröskelvärdena och processen för aktivering av åtgärd,
- c) rutiner för att möjliggöra leverans av produkter och tjänster enligt förutbestämd kapacitet,
- d) uppgifter för hantering av de omedelbara konsekvenserna av ett avbrott med lämpligt beaktande av
 - 1) människors liv och hälsa,
 - 2) förebyggande av ytterligare förluster eller avbrott i prioriterade aktiviteter,
 - 3) påverkan på miljön.

8.4.4.3 Varje kontinuitetsplan ska inkludera

- a) syfte, omfattning och mål,
- b) roller och ansvar för det team som ska tillämpa planen,
- c) åtgärder för att införa lösningarna,
- d) stödinformation som behövs för att aktivera (inklusive kriterier för aktivering), utföra, samordna och kommunicera teamens åtgärder,

SS 22304:2023 (sv)

- e) interna och externa inbördes beroenden,
- f) resurskrav,
- g) rapporteringskrav,
- h) en process för nedtrappning.

Varje plan ska kunna användas och vara tillgänglig vid den tidpunkt och på den plats där den behövs.

En kontinuitetsplan är dokumenterad information som vägleder organisationen att hantera avbrott i leveransen av produkter och tjänster.

Kontinuitetsplaner kan upprättas på olika nivåer där separata planer kan upprättas för olika aktiviteter, resurser, system, avdelningar och verksamheter. En kontinuitetsplan kan t.ex. beskriva ett alternativt arbetssätt för en prioriterad aktivitet eller hur en viss nödvändig resurs kan ersättas.

Kontinuitetsplanerna bör tas fram av, eller i nära samverkan med, berörd verksamhet och personal för att säkerställa att de är anpassade till verksamheten och dess målgrupp. Kontinuitetsplaner bör vara enkla och tydliga att använda samt kommunicerade till och tillgängliga för berörda användare. Vidare bör berörd personal ha övat på innehållet i kontinuitetsplanerna som förvaras fysiskt eller finns digitalt tillgängliga för de som behöver använda dem.

En kontinuitetsplan bör innehålla följande:

- a) Syfte, omfattning och mål.
- b) Kriterier för aktivering och vem som fattar beslut om aktivering.
- c) Reservrutin – Här beskrivs alternativa arbetssätt för den prioriterade aktiviteten. Reservrutinen bör ta hänsyn till interna och externa beroenden och redovisa vilka alternativa resurser som kan användas.
- d) Återställningsrutin – Här beskrivs hur den prioriterade aktiviteten eller nödvändiga resursen kan återställas efter ett avbrott.
- e) Återgångsrutin – Här beskrivs hur organisationen återgår till ordinarie arbetssätt när aktiviteten eller resursen är återställd.

För samtliga rutiner i planen, punkterna a) till e) ovan, bör följande tydligt beskrivas:

- Roller och ansvar – vem (befattning och namn) gör vad.
- Nödvändiga kontaktuppgifter (t.ex. telefonnummer) för att kunna utföra uppgifterna.
- Vilka som behöver informeras om läget, internt och externt och hur denna rapportering sker.

Vidare bör planen innehålla namn och funktion på den som är ansvarig för underhåll av planen samt senast övning och uppdatering.

8.4.5 Återställning

Mål: Att ta fram processer för återställning av verksamheten.

Resultat: Dokumenterade processer för att återuppta och återställa verksamheten finns.

Krav från SS-EN ISO 22301:

Organisationen ska ha dokumenterade processer för att återställa och återuppta verksamheten från de tillfälliga åtgärder som vidtagits under och efter ett avbrott.

Att återta och återställa en verksamhet efter en störning innebär att det finns fastställda kriterier för när en verksamhet anses vara tillbaka i ordinarie verksamhet. Denna information finns att hämta i konsekvensanalysen, se 8.2.2, och i verksamhetens fastställda kontinuitetsmål, se 6.2.

En effektiv och balanserad återställning kan ske genom att det i verksamheten finns

- ett på förhand utpekat ansvar för att återta verksamhetens kritiska leveranser,
- avdelade resurser, personella, finansiella och materiella, för att hantera återställningen,
- en övad organisation för att hantera återställningen,
- ett utpekat sätt som på förhand anger hur återställningen utvärderas.

Processerna möjliggör återgång till ordinarie verksamhet och att man inte fortsätter arbeta utifrån tillfälliga arbetssätt längre än nödvändigt.

Processerna kan dokumenteras separat eller ingå som delar i kontinuitetsplanen.

Processerna bör innehålla förebyggande åtgärder för att förhindra att liknande avbrott inträffar igen. Dessa kan med fördel baseras på en rotorsaksanalys av avbrottet.

Processen för att återuppta verksamheten kan t.ex. innehålla följande:

- åtgärdande av skador som uppkommit på grund av avbrottet, t.ex. genom att upparbeta kontakter för reparatörer och leverantörer av utrustning,
- återställning av eventuell förlorad information från backup-system,
- skadehantering genom restvärdesräddning.

Processen för att återställa verksamheten kan t.ex. innehålla följande:

- tillbakaflytt av verksamheten till ordinarie lokaler,
- påfyllning av tömda reservlager.

8.5 Övningsprogram

Mål: Att organisationens rutiner för kontinuitetshantering är övade.

Resultat: Kontinuitetshandlingsrutiner som är förenliga med organisationens kontinuitetsmål finns.

Krav från SS-EN ISO 22301:

Organisationen ska införa och underhålla ett övningsprogram för att över tid validera effekten av sina kontinuitetsstrategier och lösningar.

Organisationen ska utföra övningar och tester som

- är i överensstämmelse med dess kontinuitetsmål,
- är baserade på lämpliga scenarion som är välplanerade med tydligt definierade syften och mål,
- utvecklar lagarbete, kompetens, självförtroende och kunskap för de som har roller att utföra vid avbrott,
- tillsammans över tid validerar dess kontinuitetsstrategier och lösningar,
- resulterar i uppföljningsrapporter efter övningar som innehåller resultat, rekommendationer och åtgärder för att införa förbättringar,
- granskas för att främja ständig förbättring,
- utförs med planerade intervall och när det sker betydande förändringar inom organisationen eller i den miljö där den verkar.

Organisationen ska agera på grundval av resultaten av dess övningar och testning för att införa ändringar och förbättringar.

Ett övningsprogram är en serie övningar för att uppfylla ett övergripande mål.

Genom att genomföra övningar är det möjligt för organisationen att under kontrollerade former identifiera, dokumentera och åtgärda brister i organisationens kontinuitetshantering. Genom att kontinuerligt öva kan organisationen utvärdera om lösningar för att förebygga, hantera och återställa efter ett avbrott är ändamålsenliga.

SS 22304:2023 (sv)

Övningar kan genomföras som övning eller test. Skillnaden mellan övning och test är att ett test har som mål att erhålla ett godkänt eller icke godkänt resultat medan en övning genomförs i syfte att träna, bedöma och förbättra organisationens prestation. Ett exempel på där test kan användas är huruvida organisationen kan upprätthålla de enligt 8.2.2 definierade målen för återställningstid.

Ett övningsprogram bör utgå från organisationens behov och kan inkludera

- en behovsanalys,
- den högsta ledningens engagemang,
- syfte och mål med övningsprogrammet,
- tydlig planering för hur, vilka typer av övningar eller tester, var och hur ofta övningarna genomförs,
- nödvändiga resurser som behövs för att genomföra övningsprogrammet, t.ex. tid, nyckelpersoner/kompetenser och budget,
- hur utvärdering av genomförda övningar och tester genomförs och hur resultat omhändertas i organisationen,
- processer för att hantera informationssäkerhet, hälsa och säkerhet med mera.

När övningsprogrammet är implementerat i organisationen kan effektiviteten av organisationens kontinuitetsplaner säkerställas. Detta kan ske genom att

- Öva organisationens kontinuitetsplaner.
- Involvera alla berörda interna och externa medarbetare och parter, det vill säga de med ansvar för de lösningar och tillvägagångssätt som övas.
- Testa implementerade kontinuitetslösningar som t.ex. lokaler, manuella och digitala verktyg, reservbatterier och arbetsplatser.
- Säkerställa återställning av teknik och telekommunikation samt omflyttning av personal.

När man planerar för och genomför övningar bör typ av övning väljas utifrån organisationens vana att öva samt syfte och mål med övningen. I tabell 10 ges exempel på olika övningsmetoder.

Tabell 10 – Exempel på olika övningsmetoder

Övningsmetod	Beskrivning
Larmövning	En larmövning syftar till att öva eller testa en upprättad larmkedja. Övningen inleds genom att larmkedjan startas och avslutas, t.ex. när samtliga har inrapporterat eller samlats på utsedd plats.
Skrivbordsövning	Inkluderar nyckelpersoner som diskuterar scenarier och används som ett verktyg för att bygga upp kompetens och stöd för en plan eller ett förfarande. Dessa nyckelpersoner ser över planer, policyer och förfaranden för att bedöma de processer och system som krävs för att agera på oönskade situationer. Problem som uppstår till följd av de övade händelserna diskuteras av deltagarna som föreslår åtgärder och beslut.
Simuleringsövning	Simulering av en händelse och verksamhet som ofta involverar flera grupper. Övningen genomförs med hjälp av regler, inspel och tillvägagångssätt som utformas för att skildra en faktisk eller förmodad verklig situation. Simuleringsövning innehåller oftast rollspel och man kan använda teknik för att engagera deltagare och skapa stress genom simulering av olika förhållanden.

8.6 Utvärdering av dokumentation och förmågor för kontinuitet

Mål: Att organisationen har ett systematiskt angreppssätt för att utvärdera tillämplighet av organisationens relevanta kontinuitetsförmågor och hur detta finns dokumenterat i organisationen.

Resultat: Systematiskt utvärderade och dokumenterade kontinuitetsförmågor finns i organisationen.

Krav från SS-EN ISO 22301:

Organisationen ska

- a) utvärdera lämplighet, tillräcklighet och verkan av dess konsekvensanalys, riskbedömning, strategier, lösningar, planer och rutiner,
- b) genomföra utvärderingar genom revisioner, analyser, övningar, tester, incidentuppföljande rapporter och utvärderingar av prestanda,
- c) utvärdera relevanta partners och leverantörers kontinuitetshanteringsförmåga,
- d) utvärdera efterlevnad av tillämpliga författningskrav, branschstandarder och överensstämmelse med den egna policyn och de egna målen för kontinuitetshantering,
- e) uppdatera dokumentation och rutiner i lämplig tid.

Dessa utvärderingar ska göras med planerade intervall, efter en incident eller aktivering och när betydande förändringar sker.

Detta avsnitt fokuserar på betydelsen av regelbunden utvärdering av organisationens egna samt relevanta partners och leverantörers förmågor när det gäller kontinuitet i syfte att säkerställa att dessa förmågor överensstämmer med ställda kontinuitetsmål och policy. Krav kopplat till utvärdering av ledningssystemets prestanda återfinns i avsnitt 9.

Förmågan bör där det är möjligt mätas genom kontroll av att kvantitativa mål uppnås och genom på förhand uppsatta indikatorer. Då minimeras så långt som möjligt risken för subjektiva bedömningar.

Utvärderingen bör tillgodose följande egenskaper i organisationens kontinuitetshantering:

- Lämplighet – att planer och rutiner är ändamålsenliga och skapar den förmåga som krävs. Detta inkluderar t.ex.:
 - o Att utsedda reservleverantörer är de bästa för uppdraget.
 - o Att utsedd personal är de med bäst kompetens och har rätt förutsättningar att hantera avbrott och störningar.
 - o Att rutinerna är begripliga och användbara
- Tillräcklighet – att analyser och styrande dokument är tillräckliga i sin omfattning med hänsyn till risker och mål och att kapaciteten motsvarar de dokumenterade behoven Detta inkluderar t.ex.:
 - o Att säkerhetskopiering av kritisk information sker med adekvata intervall.
 - o Att det finns tillräckligt med resurser för återupptagning av verksamhet inom förutbestämda tidsramar, t.ex. att reservdelar lagerförs i tillräckliga volymer.
- Verkan – att valda åtgärder är effektiva och att de kommer kunna nå avsedd effekt.

Ett bra sätt att utvärdera kontinuitetsplaners verkan är genom övning. I samband med övning av kontinuitetsplan bör följande utvärderas:

- Förstod alla vad som skulle göras?
- Var instruktionerna i planen tillräckliga för att hantera situationen?
- Kunde ansvariga göra det som står i planen, fanns rätt kompetens?
- Var planen tillgänglig för de som behövde använda den?

Utvärderingen bör även omfatta externa aktörer vars verksamhet är nödvändiga för upprätthållande av verksamheten i den omfattning det är rimligt och genomförbart. Utvärderingen bör lägga fokus på dessa aktörers leveransförmåga och förmåga att upprätthålla kontinuitet vid störningar. Utvärdering av externa partners och leverantörer bör omfatta följande:

SS 22304:2023 (sv)

- kriticiteten för den produkt eller tjänst som de tillhandahåller,
- om leverantören är den enda för den produkten eller tjänsten,
- risken för störningar i deras förmåga att leverera produkter och tjänster till organisationen,
- om leverantören har ett kontinuitetsarbete på plats,
- i vilken utsträckning leverantören redan har bedömt sina egna risker i försörjningskedjan,
- den prioritet som ni har hos leverantören (var på listan finns ni över kritiska kunder?),
- om leverantörens RTO är i linje med den beställande organisationens.

Utvärderingen bör följa upp om gällande reglering och verksamhetskrav avseende exempelvis hållbarhet, arbetsmiljö och säkerhet efterföljs. Den bör därmed särskilt beakta ändringar i sådan reglering och styrning sedan senaste utvärderingstillfället.

Det bör finnas rutiner som tillser att dokumentationen hålls uppdaterad och aktuell. Hur ofta detta bör ske beror på förändringshastigheten inom organisationen och i omvärlden, exempelvis avseende hur snabbt risker kan uppstå och förändras, eller hur snabb personalomsättningen är.

9 Utvärdering av prestanda

9.1 Övervakning, mätning, analys och utvärdering

Mål: Att säkerställa att organisationens policy och mål uppnås och att identifiera förbättringsområden i organisationens kontinuitetshantering.

Resultat: Etablerade och dokumenterade rutiner för att mäta organisationens kontinuitetsförmåga finns.

Krav från SS-EN ISO 22301:

Organisationen ska avgöra

- a) vad som behöver övervakas och mätas,
- b) vilka metoder som i tillämplig utsträckning behövs för övervakning, mätning, analys och utvärdering för att säkerställa tillförlitliga resultat,
- c) när och av vem övervakningen och mätningen ska utföras,
- d) när och av vem resultaten av övervakning och mätning ska analyseras och utvärderas.

Organisationen ska bevara lämplig dokumenterad information som visar resultaten.

Organisationen ska utvärdera prestanda och verkan av dess ledningssystem för kontinuitetshantering.

För att komma fram till vad organisationen behöver övervaka och mäta bör organisationen utgå från fastställda kontinuitetsmål, se 6.2. Är kontinuitetsmålen mätbara? Hur kan måluppfyllnad mätas?

Vidare bör organisationen övervaka prioriterade aktiviteter enligt konsekvensanalysen, se 8.2.2. Är alla resurser tillgängliga? Uppkommer några avvikelser? För exempel på metoder för och vad som bör övervakas och mätas, se tabell 11.

Tabell 11 – Exempel på metoder för vad som bör övervakas och mätas

Exempel på vad som bör övervakas och mätas	Exempel på metod för övervakning och mätning	Exempel på nyckeltal
Avvikelser från definierade kontinuitetsmål	Avvikelseberapportering	Antal avvikelser Storlek/omfattning på avvikelser
Medvetenhet om kontinuitetspolicy	Enkäter	Andel med kännedom om policy och mål
Kostnader för störningar och avbrott i förhållande till implementering av kontinuitetslösningar	Ekonomisk uppföljning	Hur ofta inträffar störningar/avvikelser/ avbrott Hur mycket kostar störningar och avbrott Hur mycket kostar implementering av kontinuitetslösningar Hur har avbrottskostnader utvecklats över tid?
Implementering av kontinuitetsplaner	Övning	Uppfyllnad av mål för återställningstid Hur ofta genomförs övningar av kontinuitetsplaner
Nya krav, t.ex. ny lagstiftning	Omvärldsbevakning	
Förändrad hotbild	Omvärldsbevakning	

Att utvärdera och övervaka kontinuitetshandlingens prestanda är en central del i att skapa förutsättningar för att ständigt förbättra organisationens kontinuitetshandling. Detta görs genom att, i planerade intervall, utvärdera resultatet från övervakningen och mätningen i syfte att säkerställa att organisationens policy och mål uppfylls och att identifiera förbättringsområden i organisationens kontinuitetshandling.

9.2 Intern revision

Mål: Att säkerställa att ledningssystemet för kontinuitet överensstämmer med kraven och fungerar på ett ändamålsenligt sätt.

Resultat: Förutsättningar för ett fungerande revisionsarbete finns.

9.2.1 Allmänt

Krav från SS-EN ISO 22301:

Organisationen ska med planerade intervall genomföra interna revisioner för att få information om huruvida ledningssystemet för kontinuitetshandling

- a) överensstämmer med
 - 1) organisationens egna krav på sitt ledningssystem för kontinuitetshandling,
 - 2) kraven i detta dokument,
- b) har införts och underhållits på ett ändamålsenligt sätt.

Syftet med intern revision är att verifiera att ledningssystemet fungerar som det ska, det vill säga att företagets arbetssätt leder till önskade resultat och de mål som är uppställda samt att alla arbetar på det sätt som man har kommit överens om. Dessutom syftar revisionen till att fånga upp olika typer av förändringar, avvikelser och förbättringsförslag.

SS 22304:2023 (sv)

Ledningssystemets ändamål har definierats under specifika förutsättningar inom organisationen och i omvärlden, vilka i sig kan förändras både hastigt och gradvis. Den interna revisionen bör därför kontrollera att ledningssystemet fortfarande är ändamålsenligt och relevant till innehåll och form. Resultatet från en intern revision bör användas som beslutsunderlag för ledningen och som ett verktyg i det ständiga förbättringsarbetet.

Intervallen för intern revision bör synkroniseras med ledningens genomgång, och med organisationens övriga förändringstakt, såsom personalomsättning, marknadsförändringar, löptid för interna utvecklingsprojekt med mera. Att genomföra intern revision av olika delar av ledningssystemet vid sådana frekvenser gör förbättringsarbetet hanterbart. Organisationens bör genomföra intern revision av hela ledningssystemet inom en treårsperiod.

9.2.2 Revisionsprogram

Krav från SS-EN ISO 22301:

Organisationen ska

- a) planera, upprätta, införa och underhålla ett eller flera revisionsprogram, vilket innefattar frekvens, metoder, ansvar, planeringskrav och rapportering som ska ta hänsyn till betydelsen av berörda processer och resultaten vid tidigare revisioner,
- b) definiera revisionskriterier och omfattning för varje revision,
- c) välja revisorer och genomföra revisioner på ett sätt som säkerställer revisionsprocessens objektivitet och oberoende,
- d) säkerställa att revisionsresultaten rapporteras till relevanta ledningsfunktioner,
- e) bevara dokumenterad information som visar genomförandet av revisionsprogram och revisionsresultat,
- f) säkerställa att eventuella nödvändiga korrigerande åtgärder vidtas, utan onödigt dröjsmål, för att eliminera fastställda avvikelser och deras orsaker,
- g) säkerställa att uppföljande revisionsåtgärder inkluderar verifiering av vidtagna åtgärder och rapportering av verifieringsresultat.

Den interna revisionen bör ske systematiskt utifrån ett fastställt revisionsprogram. Ett revisionsprogram är ett verktyg för att effektivisera internrevisionen och kan ses som en checklista så att viktiga moment inte missas.

Revisionsprogrammet bör innehålla vilka delar av ledningssystemet som den interna revisionen särskilt bör fokusera på vid respektive tillfälle och bör ta hänsyn till resultatet av tidigare genomförda revisioner. Revisionsprogrammet bör även innehålla revisionskriterier för att mäta måluppfyllnad och önskat resultat av ledningssystemet.

Revisionsprogrammet bör även innehålla ett tidsschema för när intern revision genomförs. Om intern revision genomförs en till två gånger om året och fokuserar på hur organisationen lever upp till t.ex. ett avsnitt åt gången i detta dokument, så kan det ta cirka 3 år för internrevisorerna att slutligen ha reviderat hela systemet. Revisionsprogrammet bör också innehålla extern revision, dvs. certifieringsrevisionscykler.

De frågor som organisationen söker svar på genom sitt revisionsprogram är om ledningssystemet överensstämmer med organisationens egna krav och kraven i standarden. Har ledningssystemet införts och underhållits på ett ändamålsenligt sätt? Beroende på vilket område som revideras så formuleras relevanta frågeställningar om hur ledningssystemet har tillämpats, följs de fastställda arbetssätt i form av riktlinjer, rutiner och instruktioner för kontinuitethantering? Ytterligare en typ av frågor kan vara relaterade till prestandan. Genomförs korrigerande åtgärder på ett effektivt och ändamålsenligt sätt?

Resultatet av revisionen bör rapporteras till relevanta ledningsfunktioner. Den ledningsfunktion som ansvarar för reviderat område har i uppgift att säkerställa att nödvändiga korrigerande åtgärder

genomförs för att minimera avvikelser och deras orsaker. I uppföljande aktiviteter ingår att verifiera vidtagna åtgärder och att rapportera resultaten av verifieringen.

Internrevisionen bör vara en del i att förbättra ledningssystemet för kontinuitetshantering och ge utomstående objektiv syn på verksamhetens bedrivande.

9.3 Ledningens genomgång

9.3.1 Allmänt

Krav från SS-EN ISO 22301:

Högsta ledningen ska med planerade intervall ha en genomgång av organisationens ledningssystem för kontinuitetshantering för att säkerställa systemets fortsatta lämplighet, tillräcklighet och verkan.

Ledningens genomgång bör ske planerat och regelbundet. Underlaget för genomgången bör omfatta en årscykel.

9.3.2 Underlag för ledningens genomgång

Krav från SS-EN ISO 22301:

I ledningens genomgång ska bland annat följande beaktas:

- a) status för åtgärder som beslutats vid ledningens tidigare genomgångar,
- b) förändringar i externa och interna frågor som är relevanta för ledningssystemet för kontinuitetshantering,
- c) information om ledningssystemets prestanda, innefattande trender i fråga om:
 - 1) avvikelser och korrigerande åtgärder,
 - 2) resultat från utvärdering av övervakning och mätning,
 - 3) revisionsresultat,
- d) återkoppling från berörda parter,
- e) behovet av förändringar i ledningssystemet för kontinuitetshantering, inklusive policy och mål,
- f) rutiner och resurser som skulle kunna användas i organisationen för att förbättra prestanda för och verkan av ledningssystemet,
- g) information från konsekvensanalysen och riskbedömningen,
- h) resultat från utvärderingen av dokumentation och förmågor för kontinuitetshantering, se 8.6,
- i) risker eller ärenden som inte behandlats tillräckligt i någon tidigare riskbedömning,
- j) lärdomar och åtgärder som uppkommer ur tillbud och avbrott,
- k) möjligheter till ständig förbättring.

Ett väl genomarbetat underlag inför ledningens genomgång är en förutsättning för att ledningen ges möjlighet att fatta nödvändiga beslut.

Underlaget som presenteras bör ge en bred bild av hur väl ledningssystemet fungerar och bör vara strukturerat så att det som är viktigast kommer först (det som ledningen behöver fatta beslut om).

Angående b) så kan exempel på förändringar vara ett ändrat omvärldsläge, ny lagstiftning, nya leverantörer, ny teknik med mera.

Angående i) så kan detta vara risker som inte har behandlats i erforderlig omfattning, t.ex. på grund av avsaknad av befogenhet.

SS 22304:2023 (sv)

Angående j) så kan ledningen behöva ta ställning till nya resurser eller andra förbättringsåtgärder utifrån de incidenter som inträffat och lärdomar från dessa.

9.3.3 Resultat av ledningens genomgång

Krav från SS-EN ISO 22301:

9.3.3.1 Resultat av ledningens genomgång ska inkludera beslut som rör möjligheter till ständig förbättring och behov av ändringar i ledningssystemet för kontinuitetshantering. Detta för att förbättra ledningssystemets verkan och ändamålsenlighet, avseende:

- a) variationer i omfattningen av ledningssystemet för kontinuitetshantering,
- b) uppdatering av konsekvensanalysen, riskbedömningen, strategier och lösningar för kontinuitetshantering och kontinuitetsplaner,
- c) modifiering av rutiner och styrmedel för att agera på interna eller externa händelser som skulle kunna inverka på ledningssystemet för kontinuitetshantering,
- d) hur verkan av styrmedlen mäts.

9.3.3.2 Organisationen ska bevara dokumenterad information som visar resultaten av ledningens genomgång. Den ska

- a) meddela resultaten av ledningens genomgång till relevanta berörda parter,
- b) vidta lämpliga åtgärder med anledning av dessa resultat.

Här ges ingen kompletterande vägledning då kraven anses vara självförklarande.

10 Förbättringar

10.1 Avvikelse och korrigerande åtgärd

Krav från SS-EN ISO 22301:

10.1.1 Organisationen ska fastställa möjligheter till förbättring och införa nödvändiga åtgärder för att nå de avsedda målen för dess ledningssystem för kontinuitetshantering.

10.1.2 När en avvikelse inträffar ska organisationen

- a) agera på avvikelsen och i tillämplig utsträckning
 - 1) vidta åtgärder för att styra och korrigera den,
 - 2) hantera konsekvenserna,
- b) utvärdera behovet av åtgärder för att eliminera orsak till avvikelse, så att den inte inträffar på nytt eller på annat håll, genom att
 - 1) granska avvikelsen,
 - 2) fastställa orsakerna till avvikelsen,
 - 3) undersöka om liknande avvikelser finns eller skulle kunna inträffa,
- c) vidta nödvändiga åtgärder,
- d) granska vilken verkan genomförda korrigerande åtgärder har haft,
- e) göra ändringar i ledningssystemet för kontinuitetshantering, om det är nödvändigt.

Korrigerande åtgärder ska stå i proportion till konsekvenserna av de påträffade avvikelserna.

10.1.3 Organisationen ska bevara dokumenterad information som visar

- a) arten av avvikelser och åtgärder som vidtagits i efterhand,

b) resultaten av korrigerande åtgärder.

Exempel på vanliga avvikelser:

- Någon underlät att följa en rutin på grund av att personen inte var informerad, eller på grund av avsaknad av utbildning.
- Ett system fungerade inte, t.ex. en digital anmälningsrutin var ur funktion, krånglig, ej kommunicerad med mera.
- Ledningen tar inte sitt ansvar för att hantera de avvikelser som rapporteras, så personalen anser att det är onödigt.

Det är viktigt att ta reda på rotorsaken till avvikelserna för att komma fram till rätt korrigerande åtgärd. Ofta saknas kompetensbeskrivning, ansvar för test av funktion i system med mera.

10.2 Ständig förbättring

Krav från SS-EN ISO 22301:

Organisationen ska ständigt förbättra lämpligheten, tillräckligheten och verkan av ledningssystemet för kontinuitetshantering, baserat på kvalitativa och kvantitativa mått.

Organisationen ska ta hänsyn till resultaten av analys och utvärdering samt resultaten av ledningens genomgång för att fastställa om det, som en del av den ständiga förbättringen, finns behov eller möjligheter, att vidta åtgärder gällande verksamheten eller ledningssystemet för kontinuitetshantering.

Anmärkning: Organisationen kan använda processerna i ledningssystemet för kontinuitetshantering, såsom ledarskap, planering och utvärdering av prestanda.

Exempel på framgångsfaktorer är att skapa kvalitativa och kvantitativa mätetal som verkligen går att mäta och förstå, t.ex. antal gånger som en dator hittats olåst, antalet gånger som inköp gjorts utan hänsyn till kontinuitetskrav, antal identifierade intrångsförsök. Vidare bör organisationen tillse att alla ärenden får en ansvarig person med resurser och deadline.

Mål och indikatorer som inte kan mätas bör undvikas liksom mål och indikatorer som kan mätas men som inte är tydligt kopplade till verksamheten.

Bilaga A (informativ)

Kontinuitetshantering inför och vid höjd beredskap

Vid krig eller fara för krig kan regeringen besluta om höjd beredskap i hela eller delar av Sverige. Utöver de rekommendationer som redan finns beskrivna i denna standard har nedanstående rekommendationer utarbetats för att underlätta för planering av kontinuitetshantering under höjd beredskap.

I denna bilaga ges vägledning för att kunna tillämpa ledningssystem för kontinuitet både inför och vid höjd beredskap.

Syftet med bilagan är att beskriva de ändrade förutsättningar som gäller vid höjd beredskap och vad organisationen bör känna till och förhålla sig till i en sådan situation. Vid höjd beredskap kan ett antal lagar tillämpas för att stärka Sveriges samlade försvarsförmåga. I och med att de lagarna träder i kraft får staten möjlighet att t.ex. ransonera varor och att använda privat egendom. Myndigheter samt vissa organisationer och företag organiseras om för totalförsvar.

Tabellerna nedan följer kapitelindelningen av såväl detta dokument som SS-EN ISO 22301 och visar vilka avsnitt som innehåller särskilda tilläggsrekommendationer vid höjd beredskap. Avsnitt som gråmarkeras berörs inte av några tilläggsrekommendationer.

A.1 Omfattning

Avsnitt	Rekommendation
1 Omfattning	<i>Ingen rekommendation.</i>

A.2 Normativa hänvisningar

Avsnitt	Rekommendation
2 Normativa hänvisningar	<i>Ingen rekommendation.</i>

A.3 Termer och definitioner

Avsnitt	Rekommendation
3 Termer och definitioner	<i>Ingen rekommendation.</i>

A.4 Organisationens förutsättningar

Avsnitt	Rekommendation
4 Organisationens förutsättningar	
4.1 Att förstå organisationen och dess förutsättningar	Det som skiljer kontinuitetshantering vid höjd beredskap från fredstida påfrestningar är främst följande: – Störningar kan komma att vara av en annan art då de kan vara långvariga, många och komplexa. – Legala förutsättningar förändras när lagar och regelverk kopplade till höjd beredskap aktiveras, – Verksamhetens åtaganden och mål kan komma att förändras. – tillgång till personal och andra resurser kan förändras. Olika organisationer påverkas i olika omfattning. Vissa verksamheter kommer att i samråd med myndigheter att planläggas för att genomföra vissa uppgifter vid höjd beredskap, vilka kan vara reglerade i lagstiftning, genom avtal eller andra typer av överenskommelser. Andra verksamheter kommer ha som målsättning att upprätthålla sin ordinarie verksamhet så långt som möjligt. Ytterligare andra verksamheter kommer att behöva läggas ned för att skydda eller spara på personal och resurser till Sveriges totalförsvar. Organisationen bör utgå så långt som möjligt från ordinarie målarbete, verksamhetsstyrning, kvalitetsstyrning och riskhantering för fredstida avbrott och störningar. Organisationen bör dimensionera mål och åtaganden för de ytterligare åtgärder utöver de för fredstida avbrott och störningar som vidtas. Exempel på detta kan vara – förmåga till omställning av produktion, – hot och risker med påföljder för produkt- och tjänsteflöden, – förändringar i juridiska förutsättningar.
4.2 Att förstå berörda parter behov och förväntningar	<i>Se nedan.</i>
4.2.1 Allmänt	Organisationen bör komplettera genomförd analys med berörda parter utifrån ett beslut om höjd beredskap. Exempel på dessa kan vara – Försvarsmakten, – Arbetsförmedlingen, – Transportstyrelsen, – Länsstyrelsen, – Region, – Kommun.

Avsnitt	Rekommendation
4 Organisationens förutsättningar	
4.2.2 Författningskrav	Ett regeringsbeslut om höjd beredskap innebär bland annat att krigsplacerad personal kan behöva inställa sig på sin tjänstgöringsort och vissa myndigheter organisationer och företag organiseras om för totalförsvaret. Organisationen bör undersöka vilken lagstiftning den bör känna till. Exempel på detta kan vara – lag och förordning om totalförsvaret och höjd beredskap, – lag om skyldighet för näringsidkare, arbetsmarknadsorganisationer med flera att delta i totalförsvarets planering, – förfogandelagen (ger möjligheter för staten att förfoga över privat egendom och tjänster i syfte att tillgodose totalförsvarets behov av exempelvis försörjning.), – ransoneringslag, – arbetsrättslig beredskapslag, – lag och förordning om kommuners och landstings åtgärder inför och vid extraordinära händelse i fredstid och höjd beredskap, – lag om utrymning och inkvartering med mera under höjd beredskap, – förordning om länsstyrelsernas krisberedskap och uppgifter vid höjd beredskap.
4.3 Att bestämma ledningssystemets omfattning	Vid höjd beredskap kan omfattningen av ledningssystemet behöva ändras. Detta kan t.ex. handla om vilka produkter och tjänster som organisationen tillhandahåller vid höjd beredskap. De faktorer som påverkas av höjd beredskap bör omhändertas vid implementering av ledningssystemet för kontinuitetshantering. Notera att höjd beredskap kan påverka prioritering av organisationens produkter och tjänster enligt särskilda beredskapsavtal.
4.4 Ledningssystem för kontinuitetshantering	<i>Ingen rekommendation.</i>

A.5 Ledarskap

Avsnitt	Rekommendation
5 Ledarskap	
5.1 Ledarskap och åtagande	Ett regeringsbeslut om höjd beredskap innebär en stor påverkan på organisationen och dess personal, såväl operationellt som psykosocialt. Detta medför att ledningen förväntas visa ytterligare engagemang och stöd genom mer kommunikation kring bland annat följande saker: - Hur påverkas organisationen, - Vad görs av organisationen och dess samarbetspartners, - Tydliga instruktioner om vad som förväntas från personal och leverantörer. Ledningen bör planera vilka kommunikationskanaler som bör användas vid höjd beredskap samt sprida information i flera kanaler för att säkerställa att så många som möjligt nås.
5.2.1 Upprättande av kontinuitetspolicy	Organisationen bör se över tillämpligheten i befintlig policy och vid behov komplettera befintlig policy med t.ex. - lagstadgade förpliktelser, se 4.2.2, - förändringar i syfte, - förändringar i mål, - förändringar i åtaganden, - omprioriteringar i verksamhet vid höjd beredskap.
5.2.2 Kommunikation av kontinuitetspolicy	Organisationen bör i sin kommunikation ta hänsyn till att policyförändringar kan utgöra känsliga eller säkerhetsskydds-klassificerade uppgifter.
5.3 Roller, ansvar och befogenheter	Organisationens högsta ledning bör se över så att de befogenheter och ansvar som följer befattningar i vardagen även är tillämpliga vid höjd beredskap. Organisationen bör ta hänsyn till hur befogenheterna och ansvaret kan behöva justeras utifrån de förändringar som görs gällande avsnitten - 4 Organisationens förutsättningar, - 5.2 Policy, - 6.1 Åtgärder för att hantera risker och möjligheter, - 6.2 Kontinuitetsmål och planering för att uppnå dem. I vissa fall kan det också påverka befattningsbenämningar.

A.6 Planering

Avsnitt	Rekommendation
6 Planering	
6.1 Åtgärder för att hantera risker och möjligheter	<i>Ingen rekommendation.</i>

SS 22304:2023 (sv)

Avsnitt	Rekommendation
6 Planering	
6.2 Kontinuitetsmål och planering för att uppnå dem	Organisationen bör undersöka vilka mål som behöver kompletteras eller ändras utifrån beslut om höjd beredskap. Exempel på detta kan vara – att ha kontinuitetshantering på plats som skyddar nyckeltjänster och leveranser vid höjd beredskap. – att kontinuitetsplaner revideras (datum) med hänsyn tagen till verksamhetens krav vid höjd beredskap.
6.3 Planering av förändring	Organisationen bör planera för förändringar där höjd beredskap ändrar förutsättningarna för organisationens ledningssystem. Denna planering bör samordnas med den översyn som genomförs i 9.2 Intern revision och 9.3 Ledningens genomgång.

A.7 Stöd

Avsnitt	Rekommendation
7 Stöd	
7.1 Resurser	Organisationen bör tilldela resurser så att ledningssystemet för kontinuitetshantering fungerar även under höjd beredskap. Organisationen bör i planeringen ta hänsyn så att tillgängliga resurser kan förändras vid höjd beredskap. Exempel på detta kan vara att medarbetare kan vara krigsplacerade och inte tillgängliga för den egna organisationen vid höjd beredskap.
7.2 Kompetens	Organisationen bör säkerställa att det finns kompetens och kunskap avseende vad som gäller under höjd beredskap. Exempel på detta kan vara – relevant lagstiftning, – prioritering av produkter och tjänster, – förändrade åtaganden, – skydd och bevakning.
7.3 Medvetenhet	Organisationen bör integrera särskilda rutiner vid höjd beredskap så långt som möjligt i organisationens verksamhetsstyrning, kvalitetsstyrning och riskhantering. Exempel på detta kan vara – åtgärder för god säkerhetskultur. – medvetandehöjande åtgärder, – utbildningsinsatser.

Avsnitt	Rekommendation
7 Stöd	
7.4 Kommunikation	Vid höjd beredskap bör organisationen beakta att kommunikationen kan förändras avseende exempelvis - vem – generellt ökar behovet av kommunikation med myndigheter, kommunal och regional förvaltning samt i förekommande fall med Försvarmakten, - vad – vilka beslut som fattas och varför, - hur – kanaler kan vara utslagna eller störda, - sekretess – vissa uppgifter som behöver kommuniceras kan vara känsliga eller utgöras av säkerhetsskyddsklassificerade uppgifter.
7.5 Dokumenterad information	Dokumentation som rör verksamhet vid höjd beredskap kan innehålla känsliga uppgifter som måste hanteras korrekt och skyddas. Organisationen bör undersöka vilken dokumenterad information som kan innehålla säkerhetsskyddsklassificerade uppgifter och hur dessa hanteras enligt gällande regelverk för detta. Notera att säkerhetsskyddslagstiftningen även gäller för privat verksamhet. Exempel på uppgifter som kan vara känsliga är - beslutsordning, mandat och delegering inom verksamhetens krigsorganisation, - kommunikationskanaler och kontaktpunkter mot andra berörda parter, - säkerhetsåtgärder kring ledningsfunktioner och kritisk verksamhet vid höjd beredskap.

A.8 Verksamhet

Avsnitt	Rekommendation
8 Verksamhet	
8.1 Planering och styrning av verksamheten	Höjd beredskap kan påverka vilka kriterier som blir styrande. Kriterier som är relevanta i verksamhetens styrning under normala förhållanden kan få minskad betydelse, t.ex. ekonomi. Organisationens bör i sin planering se över vilka av kriterierna som är styrande under höjd beredskap och ta hänsyn till det i sitt ordinarie kontinuitetshanteringsarbete.
8.2 Konsekvensanalys och riskbedömning	<i>Se nedan.</i>
8.2.1 Allmänt	<i>Ingen rekommendation.</i>

Avsnitt	Rekommendation
8 Verksamhet	
8.2.2 Konsekvensanalys	Höjd beredskap kan i stor grad påverka organisationens verksamhet och tillgång till resurser och därmed få stora konsekvenser. Organisationen bör komplettera konsekvensanalysen med hänsyn till dessa ändrade förutsättningar. Exempel på detta kan vara - prioritering av varor och tjänster som tillhandahålls, - förändrade acceptabla avbrottstider, - förändrade krav på leveranssäkerhet, - förändrade tidsgränser för att återuppta verksamhet, - tillgång till externa och interna resurser.
8.2.3 Riskbedömning	Vid höjd beredskap kommer antalet risker och riskkällor öka väsentligt. Organisationen bör komplettera sin riskbedömning utifrån information som delges av Försvarmakten eller annan ansvarig myndighet. Exempel på riskkällor att beakta är - tillgången till nödvändiga resurser som t.ex. personal, livsmedel och drivmedel kan begränsas t.ex. genom påverkan på organisationens leverantörer, - prioritering av resurser till totalförsvaret, t.ex. krigsplacerad personal - anläggningar som ligger nära militärt viktig infrastruktur eller försvarsviktiga verksamheter och därmed riskerar att påverkas av stridsåtgärder och väpnat angrepp, - informationssäkerhet som t.ex. ökad mängddesinformation och storskaliga cyberattacker, - att störningar kan bli mer ihållande och långvariga än i fredstid t.ex. långvariga elavbrott, störningar i finansiella system eller avbrott i elektroniska kommunikationer, sabotage och fysisk åverkan på infrastruktur och bebyggelse.
8.3 Kontinuitetstrategier och lösningar	<i>Se nedan.</i>
8.3.1 Allmänt	Vid höjd beredskap bör organisationen ta hänsyn till förändrade omständigheter. Exempel på detta kan vara - den fysiska säkerheten för personal och tillgångar, - säkerhetsskydd, - informationssäkerhet, - förändringar i resurstillgång och juridiska förutsättningar.
8.3.2 Identifiering av strategier och lösningar	Vid höjd beredskap bör organisationen väga in de förändrade omständigheterna när den utarbetar strategier och lösningar. Exempel på detta kan vara; - tillgång till transportkapacitet, - tillgång till interna och externa personella resurser, - tillgång till kritiska reservdelar.

Avsnitt	Rekommendation
8 Verksamhet	
8.3.3 Val av strategier och lösningar	Vid val av strategier och lösningar bör organisationen överväga vilka förändringar i omvärlden som kan komma att påverka val av strategier och lösningar. Exempel på detta kan vara; - påverkan på försörjningskedjor, - påverkan på kapitaltillgång, - påverkan på personaltillgång, - påverkan på energiförsörjning.
8.3.4 Resurskrav	Höjd beredskap medför speciella förutsättningar för tillgången på resurser, t.ex. genom begränsad införsel eller att resurser tas i anspråk. Organisationen bör undersöka möjliga åtgärder för att tillgodose resurskrav vid höjd beredskap. Exempel på detta kan vara - ersättningsresurser, - krigsplacering av personal, - lagring, - redundanta system, - avtal med underleverantörer.
8.3.5 Implementering av lösningar	Vid implementering av lösningar bör organisationen överväga vilka förändringar i omvärlden som kan komma att påverka implementeringen. Exempel på detta kan vara - påverkan på leverantörskedjor, - påverkan på kapitaltillgång, - påverkan på personaltillgång, - påverkan på kundkrav, - påverkan på efterfrågan.
8.4 Kontinuitetsplaner och rutiner	<i>Se nedan.</i>
8.4.1 Allmänt	Organisationen bör tydliggöra sina rutiner för förberedande kommunikationen och klargöra vilka relevanta lagar som kan gälla vid höjd beredskap och vilka allmänna ålägganden som gäller för de anställda och vad detta innebär för deras yrkesutövande.
8.4.2 Hanteringsstruktur	Organisationen bör anpassa sina metoder för att tillgodose behovet av en effektiv hanteringsstruktur även vid höjd beredskap. Detta innefattar att ta hänsyn till - lägesbild och nationella omständigheter, - behov att verifiera och utgå från korrekt information, - identifiering av falska eller inkorrekta uppgifter.

SS 22304:2023 (sv)

Avsnitt	Rekommendation
8 Verksamhet	
8.4.3 Varning och kommunikation	Informationsläget vid höjd beredskap kan vara svårtolkat, och alla informationskällor kommer inte vara tillförlitliga. Organisationen bör analysera konsekvenserna av viktiga beslut avseende vilken information de baseras på och dennas tillförlitlighet Organisationen bör ta hänsyn till att ordinarie interna och externa kommunikationsvägar inte är tillgängliga i samma utsträckning. Exempel på detta kan vara att – telefonisystem kan vara utslagna eller överbelastade, – elektronisk kommunikation är begränsad.
8.4.4 Kontinuitetsplaner	Organisationen bör komplettera sina olika kontinuitetsplaner med hänsyn till höjd beredskap genom att analysera och belysa de resurser, aktiviteter och processer som är nödvändiga för att säkerställa måluppfyllnaden vid höjd beredskap. Exempel på detta kan vara – leveransförmågan för de produkter eller tjänster som prioriteras, – andra arbetssätt, – prioritering.
8.4.5 Återställning	Organisationen bör beakta prioriteringsordning vid återställning utifrån höjd beredskap. Exempel på detta kan vara – skador och störningar i infrastruktur, – verksamhetens betydelse för andra samhällsviktiga, verksamheter och samhällets funktionalitet i stort.
8.5 Övningsprogram	Organisationen bör anpassa övningsprogrammet så att det inkluderar relevanta externa aktörer. Det kan även vara att delta i övningar som anordnas av andra aktörer. Exempel på detta kan vara – övningar tillsammans med underleverantörer, – övningar organiserade av Försvarsmakten, – övningar av det civila försvaret. Organisationen bör komplettera innehållet i övningen utifrån förutsättningar som gäller vid höjd beredskap.
8.6 Utvärdering av dokumentation och kontinuitetsförmåga	<i>Ingen rekommendation.</i>

A.9 Utvärdering av prestanda

Avsnitt	Rekommendation
9 Utvärdering av prestanda	
9.1 Övervakning, mätning, analys och utvärdering	<i>Ingen rekommendation.</i>
9.2 Intern revision	<i>Ingen rekommendation.</i>
9.3 Ledningens genomgång	<i>Ingen rekommendation.</i>

A.10 Förbättringar

Avsnitt	Rekommendation
10 Förbättringar	
10.1 Avvikelse och korrigerande åtgärd	<i>Ingen rekommendation.</i>
10.2 Ständig förbättring	<i>Ingen rekommendation.</i>

Litteraturförteckning

- [1] SS-EN ISO 9001, *Ledningssystem för kvalitet – Krav*
- [2] SS-EN ISO 14001, *Miljöledningssystem – Krav och vägledning*
- [3] SS-EN ISO 22300:2021, *Säkerhet och resiliens – Terminologi*
- [4] SS-EN ISO 22301:2019, *Säkerhet och resiliens – Ledningssystem för kontinuitetshantering – Krav*
- [5] SS-EN ISO 22313, *Säkerhet och resiliens – Ledningssystem för kontinuitetshantering – Vägledning för implementering av ISO 22301*
- [6] SS-EN ISO/IEC 27001, *Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav*
- [7] SS-ISO 31000:2018, *Riskhantering – Vägledning*
- [8] SS-ISO 31073, *Riskhantering – Terminologi*
- [9] SIS-ISO/IEC TS 17021-6, *Bedömning av överensstämmelse – Krav på organ som reviderar och certifierar ledningssystem – Del 6: Kompetenskrav för kontroll och certifiering av kontinuitetsledningssystem*
- [10] SIS-ISO/TS 22317, *Säkerhet och resiliens – Ledningssystem för kontinuitet – Vägledning för konsekvensanalys*
- [11] SIS-ISO/TS 22318, *Säkerhet och resiliens – Ledningssystem för kontinuitet – Vägledning för kontinuitet i försörjningskedjan*
- [12] SIS-ISO/TS 22332, *Säkerhet och resiliens – Ledningssystem för kontinuitetshantering – Vägledning för framtagning av planer och processer*
- [13] SIS-ISO/TS 22331, *Säkerhet och resiliens – Ledningssystem för kontinuitet – Vägledning för att välja strategi för kontinuitet*
- [14] ISO/TS 22330, *Security and resilience – Business continuity management systems – Guidelines for people aspects of business continuity*

- [15] SFS 1992:1403 Lag om totalförsvar och höjd beredskap.
- [16] SFS 2015:1053 Förordning om totalförsvar och höjd beredskap
- [17] SFS 2022:563 Förordning om ändring i förordningen (2015:1053) om totalförsvar och höjd beredskap
- [18] SFS 1978:262 Förfogandelag
- [19] SFS 1994:1724 Lag om ändring i förfogandelagen (1978:262)
- [20] SFS 1978:268 Ransoneringslag
- [21] SFS 2014:683 Lag om ändring i ransoneringslagen (1978:268)
- [22] SFS 2006:546 Lag om utrymning och inkvartering m.m. under höjd beredskap
- [23] SFS 2019:926 Lag om ändring i lagen (2006:546) om utrymning och inkvartering m.m. under höjd beredskap
- [24] SFS 1982:1004 Lag om skyldighet för näringsidkare, arbetsmarknadsorganisationer m.fl. att delta i totalförsvarsplaneringen
- [25] SFS 2019:859 Lag om ändring i lagen (1982:1004) om skyldighet för näringsidkare, arbetsmarknadsorganisationer m.fl. att delta i totalförsvarsplaneringen
- [26] SFS 1987:1262 Arbetsrättslig beredskapslag

- [27] SFS 2010:1240 Lag om ändring i arbetsrättslig beredskapslag
- [28] SFS 2006:544 Lag om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap
- [29] SFS 2020:1275 Lag om ändring i lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap
- [30] SFS 2006:637 Förordning om kommuners och landstings åtgärder inför och vid extraordinära händelse i fredstid och höjd beredskap
- [31] SFS 2019:1053 Förordning om ändring i förordningen (2006:637) om kommuners och landstings åtgärder inför och vid extraordinära händelse i fredstid och höjd beredskap
- [32] SFS 2017:870 Förordning om länsstyrelsernas krisberedskap och uppgifter inför och vid höjd beredskap
- [33] SFS 2022:569 Förordning om ändring i förordningen (2017:870) om länsstyrelsernas krisberedskap och uppgifter inför och vid höjd beredskap
- [34] SFS 2022:524 Förordning om statliga myndigheters beredskap
- [35] SFS 2023:473 Förordning om ändring i förordningen (2022:524) om statliga myndigheters beredskap

Anteckningar/Notes

Anteckningar/Notes



Globala lösningar för ett smartare samhälle

SIS är en del av ISO och CEN som är nätverk av experter som arbetar med att skapa internationella standarder. Hos oss kan aktörer ta initiativ och samverka för best practice som främjar Sveriges konkurrenskraft och ger smart och hållbar samhällsutveckling. SIS samverkar med alla delar av det svenska samhället, som till exempel industri, akademi, offentlig sektor och frivilligorganisationer.

SIS projektleder det svenska arbetet med att ta fram standarder. Vi verkar för ökat svenskt inflytande i internationella samarbeten och för att best practice sprids och tillämpas i Sverige. Vi erbjuder också utbildningar, tjänster och produkter som hjälper våra kunder att utveckla sina verksamheter och skapa samhällsnytta med hjälp av standarder.

Vill du veta mer eller bidra till att skapa smarta globala lösningar, kontakta oss per telefon eller besök **sis.se**

Svenska institutet för standarder
104 31 Stockholm
Tel 08 - 555 523 10
kundservice@sis.se
sis.se